Hand Notes
on

CYBER FRAUDS



CHITTOOR DISTRICT POLICE

ముందుమాట

మారుతున్న జీవిత శైలితోపాటు నేరాల స్వరూపం కూడా మారుతున్నది. నేటి జీవన చిత్రంలో ఆన్‌లైన్ మోసాలు సర్వసాధారణం అయిపోయాయి. ఎవరో ఒకరు ఏదో ఒక సమయంలో మోసాలకు గురి అవుతూనే ఉన్నారు. రకరకాల మార్గాలలో మోసగాళ్ళు, నేరగాళ్ళు అమాయక ప్రజల కష్టార్జితాన్ని కొల్లగొడుతున్నారు.

ఈ రకాల మోసాలను అరికట్టుటకు సమాజంలోని అన్ని తరగతుల వాళ్ళని చైతన్య పరచుటకు చిత్తూరు పోలీసు డిపార్టుమెంటువారు సైబర్ క్రైమ్స్ మీద అవగాహన కొరకు ఒక భారీ సెమినార్ ప్రారంభించనున్నారు.

భారత ప్రభుత్వం సైబర్ క్రైమ్స్‌ను అరికట్టుటకు ఐ.యస్.ఈ.ఏ. ప్రాజెక్టును లాంచ్ చేసి ఉన్నది. ఈ ప్రాజెక్టులో భాగంగా జిల్లాలో బ్యాంకర్స్, ప్రజలను, టీచర్స్, పోలీసులకు సైబర్ క్రైమ్స్, సెక్యూరిటీ మీద అవగాహన కలిగించుటకు సి.డి.ఏ.సి., హైదరాబాదు వారితో కలిసి ఒక బాలీ సదస్సు నిర్వహించనున్నట్లు తెలిపారు.

ఇందులో భాగంగా ప్రతి హైస్కూల్, కళాశాల నుండి ఒక టీచర్, లెక్చరర్, ప్రతి బ్యాంకు నుండి ఒక బ్యాంకు అధికారి, ప్రతి పోలీస్ స్టేషన్ నుండి ఒక యస్.ఐ., ఛాంబర్ ఆఫ్ కామర్స్ సభ్యులతో ఒక రోజు అవగాహన కార్యక్రమము నిర్వహించి వారి ద్వారా ఆ తరువాత జిల్లా వ్యాప్తంగా "సైబర్ క్రైమ్ అవగాహనా వారం" జరిపి సమాజములోని అన్ని తరగతుల ప్రజలను చైతన్య పరచడం జరుగుతుంది.

ఇందుకోసం శిక్షకులకు అవగాహన కొరకు ఈ పుస్తకాన్ని రూపొందించి ముద్రించడం జరిగింది. దీనిని చదివి సైబర్ నేరాలపై అవగాహన పెంచుకోవలసినదిగా కోరుతున్నాను.

ఇట్లు

విక్రాంత్ పాటిల్, ఐ.పి.యస్.

యస్.పి., చిత్తూరు.

విషయసూచిక

1. గుర్తింపు దొంగతనం

(Identity Theft)

ఇంతకీ గుర్తింపు దొంగతనం అంటే ఏమిటి?

నగదు దొంగతనం విన్నాము... నగల దొంగతనం విన్నాము... కానీ ఈ గుర్తింపు దొంగతనం ఏమిటి అని బుర్ర గోక్కోకండి... మనకు తెలియకుండానే మన సమాచారాన్ని దొంగిలించి, వాటిని స్వార్థప్రయోజనాలకోసం దుర్వినియోగం చేయడమే గుర్తింపు దొంగతనం.

అది అనేక రూపాల్లో ఉండవచ్చు. మనకు తెలియకుండానే మనలో చాలామంది ఇలా గుర్తింపు దొంగతనం బాధితులేనంటే మీరు నమ్ముతారా?

సింపుల్‌గా ఒక ఉదాహరణ చెప్పుకుందాం...

మీరు ఒక సిమ్‌కార్డు కోసం సిమ్‌కార్డుల విక్రేత వద్దకు వెళ్ళారు. మామూలుగా మీ సిమ్‌కార్డుకు మీ గుర్తింపు పత్రం, చిరునామా ధృవీకరణ పత్రం, ఒక ఫోటో ఉంటే సరిపోతుంది. కానీ సదరు దుకాణదారు మీ వద్ద నుండి రెండు లేదా మూడు పాస్‌పోర్ట్ ఫోటోలు తీసుకున్నాడు.

మిమ్మల్ని పంపించేసి మీరిచ్చిన ధృవీకరణ పత్రాలను డూప్లికేట్ చేసి మరి కొన్ని చేసుకున్నాడు. వాటి సాయంతో దరఖాస్తులను నింపి, మీ పేరిట సంతకాన్ని తానే పెట్టి మరికొన్ని సిమ్‌కార్డులను సంపాదించి బ్లాకులో అమ్ముకున్నాడు... అదే గుర్తింపు దొంగతనం.

అలా సంపాదించి బ్లాకులో అమ్ముకున్న సదరు సిమ్‌కార్డులు ఏమైనా సంఘ విద్రోహ శక్తుల చేతి చిక్కితే? వాటిని సదరు వ్యక్తులు దేశద్రోహం కోసమో... ఆర్థిక నేరాలకో, లైంగిక నేరాలకో వాడుకోవచ్చు. పని ముగిసిపోగానే ఆ సిమ్ కార్డులను పారవేయవచ్చు.

పోలీసుల విచారణలో మీ సిమ్‌కార్డు వివరాలేమో మీ పేరిట ఉంటాయి. దాంతో వారు మీ ఇంటికి వచ్చి మిమ్మల్ని విచారణ పేరుతో వేధించవచ్చు. లేదా మీరు తీసుకోని అప్పును, క్రెడిట్ కార్డు బిల్లులను... చెల్లించాలంటూ బ్యాంకుల నుండి నోటీసులు రావచ్చు.

అమ్మాయిలను వేధిస్తున్నారని మిమ్మల్ని పోలీసులు స్టేషన్‌కు తీసుకెళ్ళవచ్చు. మీ ఆదాయపు పత్రాల రిటర్నులులను సంగ్రహించి వాటితో మీ పేరిట క్రిమినల్స్ రీఫండులు పొందవచ్చు.

మనలో చాలామంది తమకు సంబంధించిన వ్యక్తిగత సమాచారాన్ని కూడా ఫేస్‌బుక్, ట్విట్టర్ లాంటి సామాజిక వెబ్‌సైట్లలో పెట్టేస్తున్నారు. ఇదే దొంగలకు స్వయంగా తాళం చెవులను తీసుకెళ్ళి మనంతట మనమే ఇవ్వడం లాంటిదానితో సమానం.

మనకు ఆధార్ కార్డు ఎలాగో, అమెరికా లాంటి దేశాలలో సామాజిక భద్రత సంఖ్య వాడుకలో ఉంది. రెండు దాదాపుగా సమానమే. సో... మీరు ముందుగా ఏ వెబ్‌సైట్లలోనైనా మీ ఆధార్ కార్డు సంఖ్యలాంటి వాటిని అప్‌డేట్ చేయవద్దు.

2. OTP మోసాలు

హలో... మీ కార్డు బ్లాక్ అవబోతోంది... మీ సెల్‌కు ఓటీపీ నెంబర్ వచ్చింది. అది చెప్తారా...? అంటూ నమ్మకంగా ఫోన్‌లో అడుగుతారు. కాస్త ఆదమరిచి చెప్పేస్తే ఇక అంతే సంగతులు. మన అకౌంట్‌లో ఉన్న డబ్బులు కాస్తా మాయం అయిపోతాయి. సైబర్ నేరగాళ్ళు క్షణాల్లో ఆ డబ్బును కొట్టేస్తారు.

సాంకేతిక పరిజ్ఞానం కారణంగా ప్రస్తుతం అత్యధిక మంది నెట్, మొబైల్ బ్యాంకింగ్ సదుపాయాలను కలిగి ఉంటున్నారు.

బ్యాంకులు కూడా ఖాతాదారులకు ఏటీఎం డెబిట్ కార్డులను అందిస్తున్నాయి. పెట్రోల్ బంక్ మొదలు షాపింగ్ మాల్ వరకు ఏది కొనుగోలు చేసినా ఏటీఎం, డెబిట్‌కార్డుతో స్వైపింగ్ చేస్తున్నారు.

మోసం జరుగుతోందిలా...:

ఏదైనా ఆన్‌లైన్ షాపింగ్ చేసినట్లయితే తమకు నచ్చిన వస్తువులు ఎంపిక చేసుకున్న తరువాత తమ బ్యాంకు ఖాతా నెంబరుతో పాస్‌వర్డ్‌ను ఎంటర్ చేయాల్సి ఉంటుంది. ఆ సమయంలో సంబంధిత ఖాతాదారుడి సెల్‌ఫోన్‌కు ఓటీపీ నెంబరు వస్తుంది.

దానిని కొద్ది సమయంలోనే ఆన్‌లైన్‌లో ఎంటర్ చేయాల్సిఉంటుంది. తద్వారా ఒకరి బ్యాంకు ఖాతా నెంబర్, పాస్‌వర్డ్ వేరొకరు తస్కరించినప్పటికీ వాటి ఆధారంగా షాపింగ్ చేయడం సాధ్యం కాదు.

అయితే ఖాతాదారులకు దీనిపై అవగాహన లేకపోవడం, కొంతమందికి అవగాహన ఉన్నప్పటికీ అపరిచిత వ్యక్తులు చెప్పే మాటలకు ఏ మాత్రం ఆలోచించకపోవడంతో ఇటువంటి నేరాలు పెరుగుతున్నాయి.

దీంతో సైబర్ నేరాలు రెచ్చిపోతున్నారు. బ్యాంకుల నుంచి మాట్లాడుతున్నామంటూ ఖాతా, ఓటీపీ నెంబర్లు అడిగి వారి ఖాతాలోని సొమ్మును లూటీ చేస్తున్నారు. గడిచిన రెండేళ్ళుగా జిల్లాలో ఈ తరహాలో నేరాలు ఎక్కువగా జరుగుతున్నాయి.

ఖాతాదారుల వివరాలు సేకరణ...

బ్యాంకులు ఖాతాదారులకు ఏటీఎం కార్డులు జారీ, రెన్యువల్ ప్రక్రియను ప్రైవేటు ఏజెన్సీలకు అప్పగిస్తున్నాయి. ఈ విధంగా ఏజెన్సీల్లో పనిచేస్తున్న వారిని కొంతమంది నేరస్తులు లోబరుచుకుంటున్నారు. సులువుగా సంపాదించాలనే ఆలోచనతో వక్రమార్గం పడుతున్నారు. ఈ విధంగా బ్యాంకులో ఖాతాదారుని వివరాలు, ఫోన్ నెంబర్లతో కూడిన జాబితాలను సేకరిస్తున్నారు. ఆ జాబితా ఆధారంగా ఖాతాదారులకు ఫోన్ చేసే తాము ఫలానా బ్యాంకు నుంచి మాట్లాడుతున్నామని చెబుతున్నారు.

మీ ఖాతాను అప్‌డేట్ చేస్తున్నామనో, మీ ఖాతా బ్లాక్ కాబోతుందో చెప్పి వివరాలు తెలుసుకుని డబ్బు కాజేస్తున్నారు.

ముఖ్యంగా ఓటీపీ నెంబరును అడిగి క్షణాల్లోనే ఆన్‌లైన్‌లో ఆ మొత్తానికి వస్తువులు కొనుగోలు చేసుకుంటున్నారు.

ముఖ్యంగా ఈ సైబర్ నేరగాళ్ళు ముఠాగా ఏర్పడుతున్నారు. ఖాతాదారుల వివరాలు సేకరించడం ఒక ఎత్తైతే వారితో మాట్లాడుతుండగానే వారు చెప్పే వివరాల ఆధారంగా మరొకరు బ్యాంకింగ్ చేస్తారు.

వారు ఓటీపీ నెంబర్ చెప్పగానే మరొకరు తమ పని తాము ముగిస్తారు. ఖాతాదారుడితో ఓ వైపు సంభాషణ కొనసాగుతుండగానే అతని ఖాతాలోని నగదు క్షణాల్లో మాయం అవుతుంది.

ఈ విధంగా సైబర్ నేరగాళ్ళ సాంకేతిక పరిజ్ఞానాన్ని ఉపయోగించుకుని ప్రజలను దోపిడీ చేస్తున్నారు.

ఇవీ కొన్ని ఉదాహరణలు ...

- మీ ఏటీఎం కార్డు బ్లాక్ కాబోతోంది. దానిని నివారించేందుకు మీ సెల్‌ఫోన్‌కు వచ్చే ఓటీపీ నెంబర్ చెప్పండి అని అడుగుతారు.
- మీ క్రెడిట్ కార్డు బ్లాక్ అవుతుందని, దానిని నివారించేందుకు మీ ఫోన్‌కు వచ్చే ఓటీపీ చెప్పాలని అడుగుతారు.
- మీ ఖాతాకు ఆధార్ నెంబరు అనుసంధానం చేయాలి. ఇందుకు గాను ఖాతా నెంబరుతో పాటు ఆధార్ నెంబరు, ఏటీఎం నెంబర్లను అడిగి తెలుసుకోవడానికి ఫోన్‌లో మాట్లాడుతూనే మీ సెల్‌ఫోన్‌కు ఓటీపీ వస్తుంది, చెప్పండి అని అడుగుతారు. ఆ తర్వాత వెంటనే మీ ఖాతాలో నగదు డ్రా అయినట్లు మెసేజ్ వస్తుంది.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

Chittoor Police 9440900005

3. NOTE ON BANK ATM / OTP FRAUDS

ఈ రోజుల్లో ఏదైనా బ్యాంకులో ఖాతా కలిగివుండడం, దాని ద్వారా నగదు రహిత లావాదేవీలు జరపడం సాధారణం అయింది. బ్యాంకు ఖాతా కలిగిన వారందరూ Debit Card / ATM Card కలిగివుండడం కూడా సర్వ సాధారణం అయింది. సదరు కార్డు బ్యాంకు ఖాతాతో అనుసంధానమైవుంటుంది మరియు మీ సెల్‌ఫోన్ మరియు మీ ఆధార్ నెంబరు కూడా అనుసంధానింపబడి వుంటుంది.

ఉద్యోగస్తులు, రిటైర్డ్ ఉద్యోగస్తులు, వ్యాపారస్తులు, విద్యార్థులు, రైతులు, గృహిణులు మరియు డ్వాక్రా మహిళలు తమ అవసరాల మేరకు నగదును ATM సెంటర్ల ద్వారా తమ ATM Card ను ఉపయోగించి కావలసినంత మాత్రమే నగదు తీసుకొంటూ వుంటారు.

ATM సెంటర్లలో :

పై Card ద్వారా లావాదేవిని జరపాలంటే సదరు ATM Card ను ప్రత్యక్షముగా ATM Machine లో Swipe చేసి, పేరు అకౌంటు నెంబరు ధ్రువీకరించుకొన్న తరువాత రహస్య PIN code నెంబరు ఎంటర్ చేసిన తరువాతనే మీరు కోరిన నగదు Machine నుండి డెలివరి కాబడుతుంది.

ఈ సమయంలో మీ ఖాతా నుండి ఎంత మొత్తం విత్‌డ్రా చేయబడిందో మీ మొబైల్ ఫోనుకు ఒక మెసేజ్ బ్యాంకు ద్వారా పంపబడుతుంది. ఆ విధంగా మీ బ్యాంకు ద్వారా జరిగిన నగదు లావాదేవీలు మీ దృష్టిలో వుండి సురక్షితమైనవిగా వుంటాయి.

మొబైల్ మరియు ఇంటర్నెట్ బ్యాంకింగ్ సేవలు :

పై విధంగానే బ్యాంకులు నగదురహిత లావాదేవీలలో భాగంగా మొబైల్ బ్యాంకింగ్ మరియూ Internet బ్యాంకింగ్ సదుపాయాలు కూడా కలచేస్తున్నాయి. ఇందులో నమోదైన ఖాతాదారులు తమ మొబైల్ ఫోను మరియు ఇంటర్నెట్‌ల ద్వారా నగదు బదిలీ మరియు E-Commerce ద్వారా వస్తువుల కొనుగోళ్ళు జరుపుకోవచ్చు. కానీ సదరు లావాదేవీల సమయములో అతని సెల్‌ఫోనుకు ఒక రహస్య సంఖ్య (OTP) SMS ద్వారా పంపబడుతుంది.

ఆ రహస్య సంఖ్యను నమోదు చేస్తేనే ఆ లావాదేవి పూర్తి అవుతుంది. ఎన్ని లావాదేవీలు నడిపితే అన్నిసార్లు అన్ని విడివిడిగా (OTP) నెంబర్లు ఖాతాదారుని సెల్‌ఫోనుకు పంపబడతాయి. ఆయా లావాదేవీలలో ఆయా రహస్య సంఖ్యలను నమోదు చేస్తేనే ఆ లావాదేవి పూర్తి అవుతుంది. కావున ముఖ్యముగా గమనించవలసినది ఏమంటే ఆ రహస్య సంఖ్యను ఎవరితోను పంచుకొనరాదు. ఆ పని పూర్తి అయిన వెంటనే దానిని తొలగించవలెను.

బ్యాంకుల విధానంలో పొరపాట్లు :

బ్యాంకు అధికారులు ఎలాంటి ముందస్తు అనుమతి లేకుండానే గుడ్డిగా గంపగుత్తగా తమ వద్ద గల మొత్తం ఖాతాదారుల ఖాతాలకు “మొబైల్ మరియు ఇంటర్నెట్ బ్యాంకింగ్”

సేవలను by default enable చేయడంతో ఆ విషయం తెలియని ఖాతాదారులు గుర్తు తెలియని వ్యక్తులు ఫోను ద్వారా సంప్రదించి OTP నెంబరు సేకరించి తమ ప్రమేయం లేకుండానే తమ ఖాతాలో నుంచి పెద్దఎత్తున సొమ్ము దొంగిలిస్తుండడంతో ఖాతాదారులు మోసపోతున్నారు.

బ్యాంకు అధికారులు వెంటనే స్పందించి తక్షణం ఈ సదుపాయాన్ని అన్ని బ్యాంకు ఖాతాలకు Disable చేయాలి. వ్రాతమూలకంగా కోరిన ఖాతాదారులకు మాత్రమే పై సేవలు Enable చేయాలి. ఇలాంటి OTP సంఖ్యను సేకరించి సెల్‌ఫోను ద్వారా ఖాతాదారులను ఏమార్చి వారి ఖాతాల నుండి సొమ్మును తస్కరించే నేరాలను “OTP Frauds” అని అంటారు.

ఇటీవల కాలంలో కొందరు చోరులు బ్యాంకులకు సంబంధించిన ప్రధాన కార్యాలయంలో తాత్కాలిక ఉద్యోగులుగా పనిచేస్తూ వుండి ఆ సమయంలో ఖాతాదార్లకు సంబంధించిన ఖాతాలు, పేర్లు, వివరములు, A/C నెంబర్, ఆధార్ నెంబర్లు కల వివరాలను తస్కరిస్తారు. వాటిని అక్రమంగా Internet ద్వారా Cyber Criminals కు అమ్ముకున్నారు. దీనివలన విలువైన ఖాతాదార్ల రహస్య వివరాలు దొంగలకు తెలిసినంది.

నేరము చేయు విధానము :

నేరగాళ్ళు ఎక్కడో వేల కిలోమీటర్ల దూరంలో జార్ఖండ్, బెంగాల్, డిల్లీ రాష్ట్రలలో వుండి మొబైల్ ఫోన్ ద్వారా బ్యాంకు ఖాతాదార్లకు ఫోను చేసి, తాము బ్యాంకు Head Office నుండి ఫోన్ చేస్తున్నామని పలకరిస్తూ ఆ ఖాతాదారును పేరు పెట్టి పిలవడంతో వారు నిజమని నమ్ముతున్నారు.

ఆ తరువాత వారి బ్యాంకు అకౌంటు నెంబరు, ఆధార్ నెంబరు మరియు సెల్ నెంబరు మరియు కూడా చదివి వినిపించడంతో వారు పూర్తిగా నమ్ముతున్నారు. ఆ తరువాత, మీ బ్యాంకు ఖాతాను ఆధార్ నెంబరుతో అనుసందించాలని లేదా మీ ATM Card Update చేయాలని గాని లేకుంటే మీ ATM Card Block చేయబడుతుందని హెచ్చరిస్తారు.

ఆ మాటలు నమ్మిన ఖాతాదారులు తాము ఇప్పుడు ఏమి చేయాలని ప్రశ్నిస్తే వెంటనే మీ ATM Card పైన వున్న చివరి నాలుగు అంకెలు, కార్డు వెనుకవైపున వున్న CVV నెంబరు మరియు కార్డు Expiry Date వివరములను అడిగి తెలుసుకొంటారు.

బాధితులు చేయవలసినది :

వెంటనే మీరు జాగ్రత్త పడి మీ సమీపములోని బ్యాంకు లేదా పోలీసు స్టేషన్‌ను సందర్శించి అక్కడ జరిగిన సంగతులను మరియు మీ ఖాతా వివరాలు, మీరు పొందిన SMS ల వివరాలను తెలుపుతూ వ్రాత మూలకంగా ఫిర్యాదు చేయాలి.

బ్యాంకు అధికారులు చేయవలసినది :

ఖాతాదారుడు ఫిర్యాదు చేసిన వెంటనే సదరు బ్యాంకు అధికారి ఆ ATM Card ను తాత్కాలికముగా స్తంబింపచేసి తదుపరి ఖాతాలో మిగిలిన నగదు చోరీ కాకుండా కాపాడాలి.

అంతేకాక సదరు ఖాతాదారుని ఖాతాకు చెందిన నగదు లావాదేవిల Statementను ఖాతాదారునికి ఇచ్చి వెంటనే పోలీస్ స్టేషన్‌లో ఫిర్యాదు చేసేలా తెలియపరచాలి.

ఆ వెంటనే సదరు మోసపోయిన ఖాతాదారుని ఫిర్యాదును మరియు “Disputed Transaction Form” లను మెయిల్ ద్వారా సంబంధిత అధికారులకు తక్షణ విచారణ మరియు తదుపరి విచారణ కోసం Head Officeకు పంపుకోవాలి. వారు ఆ ఫిర్యాదును తమ సైబర్ నేరాల విభాగాలకు విచారణ నిమిత్తం పంపుతారు.

మోసపోయిన తరువాత రాబట్టు విధానం :

సాధారణంగా ప్రతి Online Transaction ద్వారా జరిపిన నగదు లావాదేవీలు 24 గంటల సమయం వరకు అవతలి వ్యక్తులకు నగదు గాని వస్తు సరఫరా గాని బట్వాడా చేయకుండా తాత్కాలికంగా నిలిపి వుంచి, ఆ కార్యకలాపం పై ఎలాంటి ఫిర్యాదు లేదు అని నిర్ధారించుకొన్న తరువాతనే అది అమలులోకి వచ్చి బట్వాడా చేయబడుతుంది.

దాని మేరకు స్పందించిన బ్యాంకు సైబర్ ఫ్రాడ్ విభాగము వారు తక్షణ పరిశోధన చేసి ఆ ఫిర్యాదు లోని విషయాలు నిజమేనని తేలితే ఆ ఖాతాదారుడు మోసపోయిన సొమ్ము ఇంకా బట్వాడా చేయని పక్షంలో ఖాతాదారుని బ్యాంకు అకౌంటుకు తిప్పి జమచేయడం జరుగుతుంది.

కావున మోసపోయిన ఖాతాదారులు ఎలాంటి ఆలస్యం చేయకుండా వెంటనే బ్యాంకు మరియు పోలీసు స్టేషన్‌లలో ఫిర్యాదు చేయాలి.

తమ ఫిర్యాదును మరియు “Disputed Transaction Form” లను Online ద్వారా సంబంధిత అధికారులకు వెళ్ళిందా లేదా అని తగు దాఖలా పొందాలి.

ఆ పిమ్మట రోజులలో తమ ఫిర్యాదుపై ఏ చర్య తీసుకున్నారో తెలుసుకొంటూ వుండాలి.

సూచనలు – జాగ్రత్తలు :

- ➢ గుర్తు తెలియని వ్యక్తులకు నేరుగా గాని ఫోన్ ద్వారా గాని మీ బ్యాంకు ఖాతా, ఆధార్ కార్డు, ATM కార్డు వివరాలు, PIN నెంబరు, CVV నెంబరు మరియు OTP నెంబరు తెలుపరాదు.
- ➢ హిందీలో గాని మరి ఏ భాషలో గాని తాము బ్యాంకు అధికారులమని మీ వివరాలు అడిగినట్లయితే మీరు ఎట్టి పరిస్థితులలో చెప్పరాదు.
- ➢ బ్యాంకు అధికారులు ఎలాంటి పరిస్థితులలోను మిమ్ములను ఫోను ద్వారా సంప్రదించరు. మోసగాళ్ళు మాత్రమే ఆ పని చేస్తారు.
- ➢ మిమ్మల్ని మోసగించిన వ్యక్తులు మీ సెల్‌ఫోను లోని SMSలను కూడా తొలగించమని కోరతారు. ఎట్టి పరిస్థితులలోను ఆ పని చేయవద్దు. అవి సాక్ష్యముగా చాలా ముఖ్యము.

- వెంటనే మీ బ్యాంకు ఖాతా మొబైల్ బ్యాంకింగ్, ఇంటర్నెట్ బ్యాంకింగ్ సేవలు Activate అయినవో లేవో తెలుసుకోండి. ఇందులో బ్యాంకువారిని సంప్రదించి అవి మీకు అవసరం లేకపోతే వాటిని వెంటనే A/C నుండి తొలగింపచేసుకోండి.
- మీ బ్యాంకు ఖాతా తప్పనిసరిగా మీ సెల్‌ఫోనుని అనుసంధానం చేసుకోండి. ఏ నగదు లావాదేవీ జరిపినా మీకు SMS ద్వారా వివరాలు తెలుస్తాయి. అట్టి మెసేజ్‌లను పరిశీలించుకోండి.
- వెంటనే మీ బ్యాంకు ఖాతా మొబైల్ బ్యాంకింగ్, ఇంటర్నెట్ బ్యాంకింగ్ సేవలు Activate అయినవో లేవో తెలుసుకోండి. ఇందులో బ్యాంకువారిని సంప్రదించి అవి మీకు అవసరం లేకపోతే వాటిని వెంటనే A/C నుండి తొలగింపచేసుకోండి.
- మీ బ్యాంకు ఖాతా తప్పనిసరిగా మీ సెల్‌ఫోనుని అనుసంధానం చేసుకోండి. ఏ నగదు లావాదేవి జరిపినా మీకు SMS ద్వారా వివరాలు తెలుస్తాయి. అట్టి మెసేజ్‌లను పరిశీలించుకోండి.



fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice



twitter.com/InfoSecAwa



http://infosecawareness.in



Dial - 100

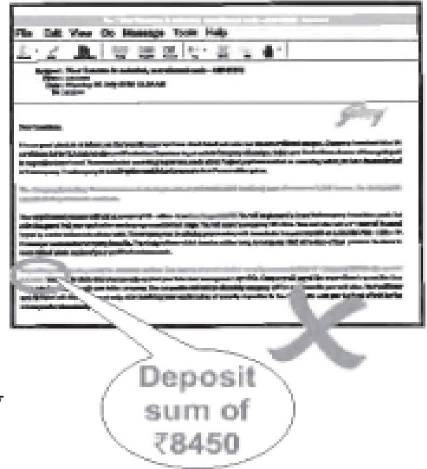
Chittoor Police 9440900005

4. ఇ-మెయిల్స్ ద్వారా వచ్చే ఉద్యోగావకాశాలపట్ల జాగ్రత్తగా ఉండండి

- చాలామంది విద్యార్థులు ఆన్‌లైన్‌లో ఉద్యోగాలకు దరఖాస్తు చేసుకుంటారు. వెబ్‌సైట్‌లలో నమోదైన వీరి వివరాలను మోసగాళ్ళు సేకరించి బూటకపు ఇ-మెయిల్స్ పంపుతుంటారు.
- ఈ ఇ-మెయిల్ కూడా నిజమైన కంపెనీలు మన మెయిల్‌లాగానే కనిపిస్తుంది. మోసగాళ్ళు బూటకపు మెయిలర్ ద్వారా ఇ-మెయిల్స్‌ను పంపి ఇంటర్వ్యూలు కూడా నిర్వహిస్తారు.
- బాధితుడికి ఉద్యోగంలో చేరమంటూ ఒక మోసపు నియామకపత్రం అందుతుంది. ఈ లేఖ అందుకున్నవారు ఒక పెద్దమొత్తం చెల్లించాలనికూడా మోసగాళ్ళు ఆ లేఖలో సూచిస్తారు.
- మోసగాళ్ళు బూటకపు మెయిలర్ సర్వీస్ ద్వారా ఉద్యోగనియామక పత్రాన్ని పంపుతారు. బహుళజాతిసంస్థ పేరుతో ఫోన్ చేయటం, ఉద్యోగ నియామకపత్రాన్ని పంపటం చేస్తుంటారు. వారి మాటలు నమ్మి ఉద్యోగార్థులు వారి ఖాతాలలో డబ్బును జమచేస్తారు. మోసగాళ్ళు వెంటనే ఆ డబ్బును విత్‌డ్రా చేసుకుంటారు.

ముందు జాగ్రత్తలు :

- స్పామ్ మెయిల్స్ ఎక్కడి నుండి వచ్చాయో సరిచూసుకోకుండా జవాబు ఇవ్వరాదు.
- అభ్యర్థులు సంస్థలతో స్వయముగా మాట్లాడ నంత వరకు డబ్బులు ఖాతాలలో జమ చేయకూడదు.
- డబ్బులు చెల్లించి ఉద్యోగాలను పొందడం వంటి ప్రక్కదారులను ప్రయత్నించకండి. అవి మోస పూరితమైనవి.
- ఉద్యోగ అవకాశాలకై సంస్థల యొక్క వెబ్‌సైట్లలో సరి చూసుకోండి.




fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

Chittoor Police 9440900005

5. సంస్థల నకిలీ ఇ-మెయిల్ ఐడీలతో జాగ్రత్తగా ఉండండి

➢ ఇ-మెయిల్స్ ద్వారా చేయు వ్యాపార లావాదేవీలకు ముందు ఇ-మెయిల్ ఐడీలోని ప్రతి అక్షరమును సరిచూసుకోండి.

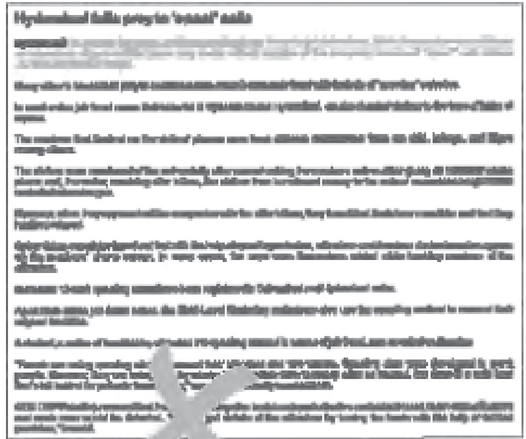
➢ నగదును సంస్థల ఖాతాలలో జమచేయు ముందు వారి ఖాతా మరియు సంస్థ పేరుల వివరములలో ఏమైనా మార్పులు ఉన్నాయేమో ఫోనులో అడిగి తెలుసుకోండి.

➢ మీ అకౌంటును తెరుచుటకు సెకెండ్ స్టెప్ వెరిఫికేషన్ కోడ్ (మొబైల్ ఎలర్ట్)ను నిర్వహించండి.

➢ ఏదైనా మోసపూరితమైనవి గమ నించినపుడు సంస్థలకు వెంటనే తెలియ పరచండి.

➢ స్పామ్ ఇ-మెయిల్స్ ఎక్కడ నుండి వచ్చాయో సరిచూసు కోకుండా ప్రత్యుత్త రము ఇవ్వకూడదు.






fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

Chittoor Police 9440900005

6. ఆన్‌లైన్ షాపింగ్ / మోసాలతో జాగ్రత్తగా ఉండండి

➢ ఇంటి వద్దనుండి ఎలక్ట్రానిక్ వస్తువులను, ఫర్నీచర్, కాస్మెటిక్స్ మరియు ఇంకా ఎన్నో వస్తువులను కొనుటకు సౌకర్యవంతమైన మరియు ప్రాచుర్యము పొందినది ఈ ఆన్‌లైన్ షాపింగ్.

దీనిద్వారా ట్రాఫిక్ మరియు రద్దీ సమస్యలను అధిగమించవచ్చు. అంతేకాకుండా షాపులు తెరుచు సమయము వరకు వేచియుండవలసిన అవసరము లేకుండా ఏ సమయములోనైనా వస్తువులను కొనవచ్చు. ఎంతో సౌలభ్యమైనదే అయినా కొన్ని ఇంటర్నెట్ ప్రమాదాలు ఉన్నాయి. ఆన్‌లైన్ షాపింగ్ చేయుటకు కొన్ని ముఖ్యమైన జాగ్రత్తలను తీసుకోవాలి.

❖ మీకు తరచుగా ఆన్‌లైన్ షాపింగ్ అలవాటు లేకపోతే ఆన్‌లైన్ షాపింగ్ చేయకండి.

❖ ఎల్లప్పుడు సెక్యూర్డ్ వెబ్‌సైట్లలోనే షాపింగ్ చేయండి

❖ ఫిషింగ్ ఇ–మెయిల్స్ / లింకులను తెరుచుట ద్వారా వారు మీ క్రెడిట్ మరియు డెబిట్ కార్డుల వివరములను తెలుసుకొని మీ అకౌంటులోని నగదును మోసపూరితంగా బదిలీ చేయవచ్చు.

ఆన్‌లైన్ షాపింగ్ చేయునప్పుడు అన్ని వివరములను చదవండి

సురక్షితమైన ఆన్‌లైన్ షాపింగ్ కొరకు కొన్ని సూచనలు :

➲ ఆన్‌లైన్ షాపింగ్‌కు ముందు మీ కంప్యూటర్లో యాంటీవైరస్, యాంటీ స్పైవేర్, ఫైర్‌వాల్ వంటి వాటితో భద్రత కలిగి వుండేటట్లు చూసుకోండి.

➲ సిస్టమ్ అప్‌డేట్‌లను మరియు వెబ్ బ్రౌజర్ సెక్యూరిటీలను కలిగి ఉండాలి.

➲ మీ కుంప్యూటర్ అత్యుత్తమ స్థాయిలో సెక్యూరిటీ కలిగివుండాలి.

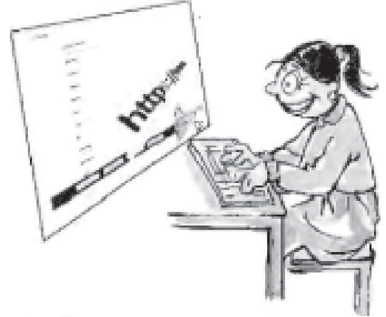
➲ ఆన్‌లైన్ షాపింగ్‌కు ముందు, ఏ వెబ్‌సైట్ల ద్వారా కొనుగోలు చేస్తున్నారో ఆ వెబ్‌సైట్ యొక్క వివరములను క్షుణ్ణంగా తెలుసుకోండి. ఎందుకంటే దాడి చేయువారి వెబ్‌సైట్లు చట్టబద్ధమైనవిగానే కనిపిస్తాయి. కాని వాస్తవానికి కావు. అందుకే అమ్మకందారుని టెలిఫోన్ నంబరు మరియు చిరునామాను నోట్ చేసుకోండి. కొనేముందు చిరునామా సరిచూసుకోండి. అంతేకాకుండా ఇతర వెబ్‌సైట్లలోని ధరలతో పోల్చిచూసుకోండి.

➲ వెబ్‌సైట్ లేదా అమ్మకందారునిపై వినియోగదారుని మరియు మీడియా యొక్క రివ్యూలను పరిశీలించండి. ఆన్‌లైన్‌లో కొనదలచితే వెబ్‌సైట్ బ్రౌజర్ అడ్రస్ బార్ లేదా స్టేటస్ బార్, https:// లేదా పాడ్‌లాక్ వంటివాటితో రక్షణ కలిగివున్నదో లేదో సరిచూసుకొని డబ్బు చెల్లించండి.

➲ కొనుగోలు పూర్తయిన తరువాత, వస్తువు యొక్క ధర వివరములు, ధృవపత్ర రసీదులను మరియు విక్రయ నిబంధనలు మరియు షరతులను ప్రింట్ లేదా స్క్రీన్‌షాట్ తీసుకొని ఉంచుకోవాలి.

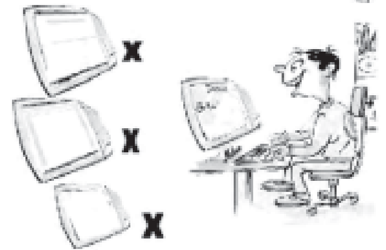
- కొనుగోలు పూర్తయిన వెంటనే మీ క్రెడిట్ కార్డు స్టేట్‌మెంటులో మీరు కట్టిన చార్జీలను సరి చూసుకోండి. ఒకవేళ మీరు కట్టిన ఛార్జీలు స్టేట్‌మెంటులో ఛార్జీలు వేరుగా ఉంటే వెంటనే సంబంధిత అధికారికి తెలియజేయండి.
- "దయచేసి మీ కొనుగోలు, చెల్లింపు మరియు ఖాతావివరములను నిర్ధారించండి" అంటూ వచ్చే ఇ–మెయిల్స్‌తో జాగ్రత్త వహించండి. చట్టబద్ధమైన వ్యాపారస్తులు ఇటువంటి ఇ–మెయిల్స్‌ను పంపించరు. మీకు ఇటువంటి ఇ–మెయిల్స్ వచ్చివుంటే వెంటనే మీకు అమ్మిన వ్యాపారికి తెలియపరచాలి.
- లావాదేవీలు పూర్తయిన వెంటనే అన్ని వెబ్ బ్రౌజరు కుక్కీలను (Cookies) తొలగించి మీ కంప్యూటరును ఆపుచేయాలి. స్పామర్లు మరియు ఫిషర్లు ఏ కంప్యూటర్లు ఇంటర్నెట్‌తో కనెక్ట్ చేయబడి వున్నాయో చూసి స్పామ్ ఇ–మెయిల్స్‌ను పంపించుటకు ప్రయత్నించి హానికర సాఫ్ట్‌వేర్ ద్వారా మీ వ్యక్తిగత సమాచారమును తెలుసు కుంటారు.





ఆన్‌లైన్ లావాదేవీలు చేయుచున్న ప్రతిసారీ మిగతా అన్ని అప్లికేషన్స్‌ను మూసేయండి







ఆన్‌లైన్ షాపింగ్ చేయునప్పుడు సరఫరా నగదుకే ప్రాముఖ్యత ఇవ్వండి



7. రుణమోసాలపట్ల జాగ్రత్తగా ఉండండి

- తక్కువ వడ్డీలకు వ్యక్తులకు రుణాలు ఇస్తామంటూ కొందరు మోసగాళ్ళు దినపత్రికలలో ఒక సెల్‌నంబర్‌తో ప్రకటనలు ఇస్తారు.

  ఆ ప్రకటనలలో ఇచ్చే సెల్ నంబర్‌ను తప్పుడు చిరునామాతో తీసుకుంటారు.

- మోసగాడు బాధితులకు రుణం మంజూరయ్యిందంటూ కొన్ని నకిలీ సర్టిఫికెట్లు పంపుతాడు.

  కొంత మొత్తాన్ని తమ బ్యాంక్ ఖాతాలలో డిపాజిట్ చేయాలంటూ సూచిస్తాడు. బాధితుడు రిజిస్ట్రేషన్, పన్నులు, న్యాయవాది ఫీజు మొదలైనవాటికోసం ఆ మొత్తాన్ని ఆ నకిలీ ఖాతాలలో డిపాజిట్ చేస్తాడు.

  నకిలీ సర్టిఫికెట్ల వల్ల అప్రమత్తంగా ఉండండి.

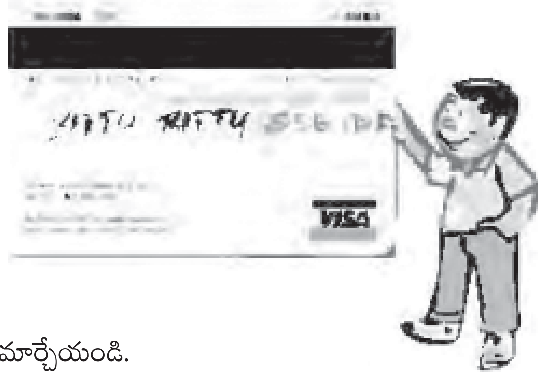
- తక్కువ వడ్డీలతో రుణాలు మంజూరు చేయిస్తామంటూ ప్రకటనలు ఇచ్చే ఆర్థిక సంస్థలను నమ్మకండి.



8. డెబిట్/క్రెడిట్ కార్డ్ మోసాలపట్ల అప్రమత్తంగా ఉండండి

క్రెడిట్ కార్డు, డెబిట్ కార్డు / ఏటీఎం కార్డు వాడుటకు ముందు తీసుకోవలసిన జాగ్రత్తలు.

- మీరు బ్యాంకు నుండి కార్డు అందుకునేముందు ఆ కవర్ మొత్తం సీల్ చేయబడి ఉన్నట్లుగా, ఎటువంటి డేమేజ్ లేకుండా ఉన్నట్లుగా నిర్ధారించుకోండి.
- మీరు బ్యాంకు నుండి కార్డు తీసుకున్న వెంటనే కార్డుపై సంతకం చేయండి.
- కార్డు వెనకాల ఉన్న చివరి మూడు అంకెల (సివివి) నంబరు మూసివుంచుటకు ప్రయత్నించండి.



- ఖాతా లావాదేవీలను సరి చూసుకోవ డానికి మీ ఫోను నంబరును వెంటనే రిజిష్టర్ చేసుకోండి.
- మీ పిన్ నెంబరును వెంటనే మార్చేయండి.

షాపింగ్ మాల్స్ మరియు రెస్టారెంట్‌లలో క్రెడిట్ / డెబిట్ కార్డులను వాడటం సురక్షితంకాదు :

- అమ్మకదారు మీ కార్డును ఎలా స్వైప్ చేస్తున్నాడనేదానిని ఒక కంట గమనిస్తుండండి.
- లావాదేవీలు ఎల్లప్పుడూ మీ ఎదుటే జరిగేటట్లు చూసుకోండి.
- ఖాళీగా ఉన్న క్రెడిట్ కార్డు రసీదుపై ఎప్పుడూ సంతకం చేయొద్దు. రసీదులో ఖాళీగా ఉన్న ప్రాంతంలో ఒక గీత గీయండి.
- రెస్టారెంట్స్ / షాపింగ్ మాల్స్‌లో ఇచ్చే సర్వే పత్రాలలో మీ వ్యక్తిగత సమాచారాన్ని ఇవ్వొద్దు.

ఇంటర్నెట్‌లో క్రెడిట్ / డెబిట్ కార్డులను సురక్షితంగా ఉపయోగించటం:

- లావాదేవీలకు, షాపింగ్‌కు ఎల్లప్పుడూ సురక్షిత వెబ్‌సైట్లను వాడండి.
- మీకు తెలిసిన, విశ్వసనీయమైన వ్యాపారులవద్దే కొనుగోలు చేయండి.
- భద్రతకు సంబంధించిన గుర్తులు న్నాయో లేదో చూడండి. మీ బ్రౌజర్ అడుగున ఒక తాళం బొమ్మ, https://తో మొదలయ్యే యూఆర్ఎల్ వంటి భద్రతా గుర్తుల (మీ ఖాతా సమాచారాన్ని కాపాడటానికి మీ కొనుగోళ్ళను ఎన్‌క్రిప్షన్‌తో భద్రపరచినట్లు ఈ గుర్తులు తెలుపుతాయి) కోసం చూడండి.

- ఫిషింగ్ మోసాలను తప్పించుకోవాలంటే ఇ–మెయిల్ మెసేజ్‌లన్నింటిని అనుమానంతో చూడండి. ఆర్థిక సమాచారంతో సహా వ్యక్తిగత సమాచారాన్ని అడిగే ఇ–మెయిల్ మెసేజ్‌లకు స్పందించకండి. బ్యాంక్‌లు అలాంటి సమాచారాన్ని కోరవు.
- మీ క్రెడిట్ / డెబిట్ కార్డుతో ఆన్‌లైన్ లావాదేవీ జరిపిన తర్వాత ఆ వెబ్‌సైట్ నుంచి వెంటనే లాగ్‌ఆఫ్ అవ్వండి మరియు బ్రౌజర్ కుకీలను (Cookies) తొలగించండి.
- పేమెంట్ సమాచారాన్ని ఇ–మెయిల్ ద్వారా ఎప్పుడూ పంపొద్దు. ఇంటర్నెట్ ద్వారా ప్రయాణించే (ఇ–మెయిల్ వంటివి) సమాచారం ఇతరులు చదవకుండా ఉండటం పూర్తిగా అసాధ్యమని చెప్పలేం.
- ఆన్‌లైన్‌లో వ్యక్తిగత సమాచారం ఇచ్చేటప్పుడు అప్రమత్తంగా ఉండండి.
- ప్రోత్సాహక పథకాల మోసాలపట్ల జాగ్రత్తగా ఉండండి. వ్యక్తిగత సమాచారాన్ని దొంగిలించేవారు ఫోన్ ఆఫర్‌లను ఉపయోగించుకుని మీ వ్యక్తిగత సమాచారాన్ని అడగొచ్చు.
- మీ పాస్‌వర్డ్‌లను రహస్యంగా ఉంచండి. కొన్ని ఆన్‌లైన్ దుకాణాల్లో కొనుగోలు చేసేముందు యూజర్ నేమ్, పాస్‌వర్డ్ నమోదు చేసుకోవాల్సిన అవసరం ఉంటుంది. మీ ఏటీఎం పిన్‌ను కాపాడుకున్నట్లే. ఈ ఆన్‌లైన్ పాస్‌వర్డ్‌లను కూడా రహస్యంగా, బయటవారికి తెలియకుండా భద్రపరుచుకోవాలి.

చేయవలసినవి :

- ☑ ఏటీఎం ఉపయోగించేముందు, కార్డు చొప్పించే ప్రదేశంలో ఏమీ ఉండకుండా చూసుకోండి. (స్కిమ్మింగ్ కాకుండా ఉండటానికి)
- ☑ లావాదేవీ చేసేటపుడు పిన్ నంబర్‌ను రహస్యంగా ఉంచండి. లావాదేవీ రసీదులను వెంట ఉంచుకోవద్దు.
- ☑ బ్యాంకులు సూచించినట్లు మీ ఏటీఎం పిన్‌ను మూడు నెలలకొకసారి మార్చండి.
- ☑ లావాదేవీలలో మోసాలకు గురికాకుండా ఉండటానికి మీ క్రెడిట్ కార్డు రసీదులను దాచివుంచండి. మీ మంత్లీ స్టేట్‌మెంట్‌తో వాటిని సరిచూసుకోండి.
- ☑ బాగా అవసరమైన క్రెడిట్ కార్డులను మాత్రమే వెంట తీసుకెళ్ళండి.
- ☑ మీ క్రెడిట్ కార్డు నంబర్ ఉన్న రసీదులను చించేయండి.
- ☑ మీ అడ్రస్ మారినట్లయితే, క్రెడిట్ కార్డు ఇచ్చిన బ్యాంకులకు ముందే తెలియజేయండి.
- ☑ మీ క్రెడిట్‌కార్డు పోయినట్లయితే వెంటనే ఆ విషయాన్ని తెలియజేయండి.
- ☑ రెన్యూవల్ / అప్‌గ్రెడిషన్ సమయంలో మీ కార్డును పారవేయాలనుకుంటే ముందు దానిని అడ్డంగా కత్తిరించి పారవేయండి.

చేయవలసినవి :

- ☒ బ్యాంక్‌నుంచి కార్డు వచ్చిన కవర్ చిరిగిపోయివున్నా, సీల్ తెరిచి ఉన్నా దానిని స్వీకరించొద్దు.

- ☒ మీ క్రెడిట్ కార్డుపై పిన్ నంబర్ రాయొద్దు.
- ☒ మీరు అరుదుగా ఉపయోగించే అదనపు క్రెడిట్ కార్డులను వెంట తీసుకెళ్ళొద్దు.
- ☒ మీ క్రెడిట్ కార్డు నంబర్ / ఏటీఎం పిన్‌ను ఎవరికీ తెలపొద్దు. బ్యాంక్ ప్రతినిధులమని ఎవరైనా చెప్పినా కూడా మీ కార్డును ఎవరికీ ఇవ్వొద్దు.
- ☒ ఏటీఎం మెషిన్‌ను ఉపయోగించడంలో సాయపడతామని కొత్తవారెవరైనా ముందుకొస్తే, వారి సాయాన్ని తీసుకోవద్దు.
- ☒ ఏటీఎం మెషిన్ సరిగా పనిచేయకపోతే దానిని ఉపయోగించొద్దు.
- ☒ మీ ఖాతా వివరాలను తెలియనివారు / ధృవీకరించబడినవారికి బదిలీ చేయొద్దు, పంచుకోవద్దు.
- ☒ అందరూ ఉపయోగించే ఇంటర్నెట్ సెంటర్ల వంటి కంప్యూటర్లలో మీ క్రెడిట్ / డెబిట్ కార్డులను ఉపయోగించి నెట్ బ్యాంకింగ్ లేదా ఆన్‌లైన్ పేమెంట్లు చేయొద్దు.
- ☒ మీరు ఊహించని చోట్లనుంచి వచ్చే ఇ–మెయిల్ ఎటాచ్‌మెంట్లను, ఇన్‌స్టంట్ మెసేజ్ డౌన్‌లోడ్ లింక్‌లను ఓపెన్ చేయొద్దు. అనుమానాస్పద ఇ–మెయిల్‌లను వెంటనే తొలగించండి.
- ☒ ఫోన్ చేసింది మీరే అయితే గానీ, ఆ కంపెనీ మంచిదని మీకు తెలిస్తేనే గానీ మీ ఖాతా వివరాలను ఫోన్‌లో చెప్పొద్దు. మీరు ఫోన్ అందుకున్నప్పుడు మీరు క్రెడిట్ కార్డు సమాచారాన్ని బయటకు చెప్పొద్దు (దీనినే విషింగ్ అంటారు).
- ☒ సురక్షితంగాని వెబ్‌సైట్‌లో మీ క్రెడిట్ కార్డు సమాచారాన్ని ఇవ్వొద్దు.
- ☒ ఆదాయపు పన్నుశాఖ, రిజర్వ్ బ్యాంకు వంటి ప్రభుత్వ అధికారులు, వీసా లేక మాస్టర్ కార్డు వంటి ఏదైనా కార్డులు ఇచ్చే సంస్థ ప్రతినిధులు ఇ–మెయిల్ ద్వారా కోరినా కూడా మీ పాస్‌వర్డ్, కస్టమర్ ఐడీ, డెబిట్ కార్డు నంబర్, పిన్ సీవీవీ, జన్మదిన తేదీ వంటి కీలక సమాచారాన్ని ఇవ్వొద్దు.
- ☒ మీ బ్యాంకు ఖాతా సమస్యలను గానీ, మీ ఖాతా వివరాలనుగానీ, పాస్‌వర్డ్‌నుగానీ సోషల్ నెట్‌వర్కింగ్ సైట్‌లో లేదా బ్లాగ్‌లో ప్రస్తావించొద్దు.
- ☒ ఏటీఎం పిన్ వంటి కీలక సమాచారాన్ని మీ మొబైల్ ఫోన్‌లో పెట్టొద్దు.



మీ క్రెడిట్ కార్డు మరియు పిన్‌ను ఒకేచోట ఎప్పుడూ ఉంచకండి

9. సైబర్ స్పేస్‌లో తీసుకోవలసిన నివారణ చర్యలు

➢ మీ వ్యక్తిగత వివరములను ఇవ్వకండి: ప్రయాణాల తేదీలను, మీరు చూచుటకు వెళుతున్న సినిమా సమయము మరియు స్థల వివరములు, సాయంత్ర వేళ వెళ్ళు క్లాసుల వివరములు మొదలగు మీ వ్యక్తిగత వివరములను ఆన్‌లైన్‌లో ఇవ్వకూడదు.

➢ మీ వ్యక్తిగత వివరములను రహస్యముగా ఉంచండి. పరిచయము లేనివారితో జాగ్రత్త.

➢ స్నేహితులు పరిచయస్తులు కాని వ్యక్తులతో స్నేహము కొరకు విన్నపములను మరియు మీ వ్యక్తిగత వివరములను ఇచ్చుటకు తిరస్కరించండి. సంబంధాలు బెడిసినప్పుడు దూషించు మరియు అసభ్యకర సందేశములను పంపవచ్చు.

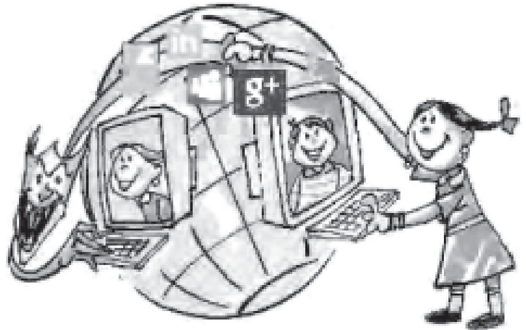
క్రింది ప్రమాదములతో జాగ్రత్త :



స్పామ్ : స్పామ్ అంటే ఏదైనా వస్తువు గురించి ను ఇ–మెయిల్‌లిస్టుకు లేదా ఇ–మెయిల్ గ్రూపులకు పంపు అనవసర ఇ–మెయిల్ ప్రకటనలు. అలాగే స్పామర్స్ కూడా అనవసర ఇ–మెయిల్స్‌ను ఉచిత సోషల్ నెట్‌వర్కింగ్ సైట్లను వినియోగించి కొన్ని బిలియన్ల వినియోగదారులకు, స్పామర్లు సులభంగా వారి వ్యక్తిగత సమాచారమును సేకరించి పంపుచున్నారు.

అప్‌డేట్ చేసిన స్పామ్–బ్లాకింగ్ సాఫ్ట్‌వేర్‌నే ఎల్లప్పుడూ ఉపయోగించండి

స్కామ్స్ : సాధారణంగా ఆన్‌లైన్ స్కామర్స్ వినియోగదారులను కొత్త ఫాలోవర్స్‌ను జతచేసుకొనుటకు వ్యక్తిగత వివరములకై అడుగుచూ లింకుతో ఉన్న ఇ–మెయిల్ లేదా సందేశములను పంపుతారు. ఈ లింకులు అప్లికేషన్స్, గేమ్స్ మొదలగునటువంటి వాటిలాగా ఉంటాయి.



ఎప్పుడైనా వినియోగదారుడు తమ వ్యక్తిగత వివరములను ఈ లింకులకు పంపిన వెంటనే స్కామర్స్ ఆ వివరములను తీసుకొని దుర్వినియోగపరచవచ్చు.

హానికర అప్లికేషన్స్ : హానికర అప్లికేషన్స్, వివిధ అప్లికేషన్స్‌ను వినియోగించునప్పుడు లేదా సాఫ్ట్‌వేర్ ఇన్ఫర్మేషన్ అప్పుడు రావచ్చు. అప్లికేషన్ ఇన్‌స్టలేషన్ మొదలుపెట్టుటకు, లేదా వీడియోలను వీక్షించుటకు లింకులు మొదలగువాటికై సోషల్ నెట్‌వర్కింగ్ అప్లికేషన్స్‌పై క్లిక్ చేస్తే, మీరు అడిగిన అప్లికేషన్స్‌ను మొదలుపెట్టుటకు మీ మౌలిక సమాచారమును, మీ వాల్ అప్‌డేట్, వాల్‌పై పోస్టు చేయుటకు వారికి వీలు కల్పించవలసిందిగా అడుగుతూ, ఇటువంటి హానికర అప్లికేషన్స్ రావచ్చు.

క్లిక్ జాకింగ్: ఇంటర్నెట్ వాడకందారు ప్రమాదరహిత వెబ్‌పేజీలపై క్లిక్ చేస్తున్న సమయంలో వారిని తప్పుదోవ పట్టించి వారి రహస్యసమాచారాన్ని రాబట్టుకోవడం, ఆ కంప్యూటర్‌ను తమ అధీనంలోకి తీసుకోవడ అనే మోసాన్ని క్లిక్ జాకింగ్ అంటారు. అనేక బ్రౌజర్లు, ప్లాట్‌ఫామ్‌లు క్లిక్‌జాకింగ్‌కు అనువుగా ఉన్నాయి. వాడకందారుకు తెలియకుండానే నడిచే ఎంబెడెడ్ కోడ్ లేదా స్క్రిప్ట్‌ద్వారా క్లిక్‌జాకింగ్ జరుగుతుంది. ఇది సోషల్ నెట్‌వర్కింగ్ డొమైన్‌లో కూడా జరుగుతుంటుంది. వాడకదారులతో కొన్ని లింక్‌లు, ఐపీస్‌లు, బటన్‌లు మొదలైనవాటిపై క్లిక్ చేయించటం ద్వారా వారికి తెలియకుండా వారే హానికరమైన పనులు చేసేటట్లు చేయడం ఈ చర్య వెనక ఉన్న లక్ష్యం.

ఫిషింగ్ : అసలు వెబ్‌సైట్‌లాగానే నకిలీ సైట్‌ను సృష్టించటాన్ని ఫిషింగ్ అంటారన్నది అందరికీ తెలిసిన విషయమే. బ్యాంకులు, సుప్రసిద్ధ వాణిజ్య వెబ్‌సైట్లపై చేసినట్లుగానే సోషల్ నెట్‌వర్కింగ్‌లో కూడా ఇప్పుడు ఫిషింగ్ జరుగుతోంది. ప్రత్యేకమైన థీమ్‌లు అందిస్తున్నామని, ప్రొఫైల్ అప్‌డేట్ చేసుకోమని, సెక్యూరిటీ అప్లికేషన్ / ఫీచర్స్ అప్‌డేట్ చేసుకోమని తెలుపుతూ బూటకపు ఇ-మెయిల్స్, సందేశాలు పంపటం సోషల్ నెట్‌వర్కింగ్‌లో జరిగే ఫిషింగ్. ఆ అప్‌డేట్స్ చూడటానికి నెట్ వాడకందారు ఒక లింక్‌ను అనుసరించి లాగిన్ అవ్వాల్సివుంటుంది. అప్పుడు వారి వివరాలను మోసగాళ్ళు సేకరిస్తారు. అసలు లాగిన్‌పేజీకి నకలుగా సృష్టించబడిన ఆ లింక్‌పేజీ రహస్య సమాచారాన్ని సేకరించటానికి ఉద్ధేశించబడినది.



ఫిషింగ్ ఇ-మెయిల్ స్కామ్స్ నుండి అప్రమత్తంగా ఉండండి

మార్గదర్శకాలు :

➲ మీ పేరు, ఇంటి / పాఠశాల చిరునామా, ఫోన్ నంబర్లు, వయస్సు, లింగం, క్రెడిట్ కార్డు వివరాలు వంటి వ్యక్తిగత సమాచారాన్ని ఎప్పుడు ఇవ్వొద్దు, పోస్టు చేయొద్దు.

➲ ఇంటర్నెట్ అనేది ప్రపంచంలోని అతిపెద్ద సమాచార మార్పిడి సాధనం కాబట్టి మీరు ఆన్‌లైన్‌లో పోస్టు చేసే సమాచారాన్ని ఆన్‌లైన్‌లో ఉన్న ప్రతిఒక్కరూ చూడొచ్చు. మీరు వాడుతున్న వెబ్‌సైట్‌నే వాడే ఇతరులు మీరు పోస్టు చేసిన సమాచారాన్ని, మీ ప్రొఫైల్‌ను తెలుసుకోవచ్చు. మీ అకౌంటును చూపేవారిలో మీ తల్లిదండ్రులు, స్నేహితులు, టీచర్లు వంటి మంచివారితో పాటు అపరిచితులైన చెడ్డవారు కూడా ఉంటారు.

➲ మీరు వెబ్‌సైట్‌లో ఇచ్చిన సమాచారము మిమ్మల్ని ఇరికించడానికి కూడా ఉపయోగపడే అవకాశం ఉన్నదని గుర్తుంచుకోండి.

- మీ పాస్‌వర్డ్‌ను మీ తల్లిదండ్రులకు లేదా సంరక్షకులకు తప్ప ఇంకెవరికి ఇవ్వరాదు.
- మీ పాస్‌వర్డ్‌ను తరచుగా మార్చుతూ ఉండండి మరియు తిరిగి సోషల్ నెట్‌వర్కింగ్ సైట్లకు పంపే లింకులపై క్లిక్ చేయకండి. మీరు తిరిగి మీ అకౌంటులోకి వెళ్ళుటకు బ్రౌసర్లలో టైపు చేయండి లేదా మీరు సేవ్ చేసిన బుక్‌మార్క్‌ను ఉపయోగించండి.
- సోషల్ నెట్‌వర్క్ సైట్లను ఎన్నుకున్నప్పుడు గోప్య వివాదాస్పద అంశాలను పరిశీలించాలి.
- సోషల్ నెట్‌వర్కింగ్ సైట్లలో స్నేహితులను జతపరుచుకునేటప్పుడు మీకు తెలిసినవారిని మాత్రమే అంగీకరించండి.
- ఎప్పుడూ కూడా సోషల్ నెట్‌వర్కింగ్ సైట్లలో పరిచయమైన వ్యక్తులను కలిసే ముందు మీ తల్లిదండ్రుల అంగీకారమును పొందండి.
- సోషల్ నెట్‌వర్కింగ్ సైట్లు వాడకందారులు తమ సమాచారాన్ని ఎవరెవరు చూడొచ్చని నియంత్రించుకోటానికి అవకాశాలు కలిగిస్తున్నాయి. ఈ సౌలభ్యాలను వినియోగించుకోండి.
- మీ కుటుంబ గౌరవాన్ని భంగపరిచే టాపిక్‌లను రాయకండి.
- సోషల్ నెట్‌వర్కింగ్ సైట్లలో పరిచయములేని వ్యక్తులను మీ ఫోటోలను, వీడియోలను మరే ఇతర సున్నితమైన సమాచారమును పంపవద్దు.
- సోషల్ నెట్‌వర్కింగ్ అకౌంటు నుండి మీ సమాచారమును మార్చినా లేక దొంగలించబడినా వెంటనే సోషల్ నెట్‌వర్కింగ్ సపోర్ట్ టీంకు తెలియజేయండి.
- మీ ప్రొఫైల్‌లో ఎవరైనా పరుషమైన లేదా బాధకలిగించు విధంగా పోస్టులు రాస్తే స్పందించకండి.
- అనవసరమైన విమర్శలను పంపించి స్నేహితులను లేదా సందేశాలను తొలగించి ఈ విమర్శలను నెట్‌వర్కింగ్ సైట్లకు తెలియజేయండి.
- మీ స్నేహితుల వివరాలను నెట్‌వర్కింగ్ సైట్లలో పోస్టుచేయకండి. అది వారిని ఇబ్బందికి గురిచేయవచ్చు. వారి గ్రూపు ఫోటోలను, స్కూలు పేరును, చిరునామాలను, వయసు మొదలగునవి పోస్టుచేయకుండా వారిని సంరక్షించండి.
- నెట్‌వర్కింగ్ సైట్లలో మీరు చేయబోవు పనులను పోస్టు చేయకండి.
- నెట్‌వర్కింగ్ సైట్లలోని సెట్టింగులను పరిశీలించి, మీరు స్నేహితులుగా అంగీకరించిన వ్యక్తులు మాత్రమే జరపరుచుకొనేలా సెట్ చేయండి మరియు మీరు స్నేహితులుగా అంగీకరించిన వ్యక్తులు మాత్రమే మీ ప్రొఫైల్ వీక్షించేలా సెట్ చేయండి.

(కౌన్ బనేగా కరోడ్‌పతి, ఎయిర్‌టెల్ లాటరీ, టాటా డొకోమో లాటరీ, స్టార్ స్పోర్ట్స్ లాటరీ, ఎయిర్‌టెల్ / ఐసీసీ కప్ లాటరీ, బీబీసీ / హీరోహోండా/ స్టార్ లాటరీ / స్టార్ క్రికెట్ లాటరీ/ స్పోర్ట్స్ / షెవర్లే మోటార్స్ మొదలైనవి)

10. పైన పేర్కొన్నటువంటి లాటరీ ఇ-మెయిల్స్/ ఎస్ఎంఎస్‌లు వస్తున్నాయా?



➢ లాటరీ ఇ-మెయిల్స్ / ఎస్ఎంఎస్‌లలో మోసగాళ్ళు ప్రజలను – మీ సెల్ నంబర్‌కు లక్షల్లో లాటరీ తగిలిందని, ఫలానా ఈమెయిల్ ఐడీకి మీ సమాచారాన్ని ఇవ్వాలని కోరుతూ ఇ-మెయిల్, ఎస్ఎంఎస్ లేదా ఫోన్ కాల్ ద్వారా సంప్రదిస్తారు.

➢ బాధితుడు అది నిజమేనని నమ్మి ఇ-మెయిల్ ద్వారా తన పూర్తి వివరాలను ఇ-మెయిల్ ద్వారా తెలియజేస్తాడు.

➢ మోసగాళ్ళు బాధితుడి పేరుమీద రూపొందించిన నకిలీ చెక్ / సర్టిఫికెట్ యొక్క స్కాన్ చేయబడిన కాపీని మెయిల్ చేస్తారు. రిజిస్ట్రేషన్ రుసుము కింద నిర్ధిష్టమొత్తాన్ని జమచేయమంటూ బాధితుడికి ఒక బూటకపు ఖాతా నంబర్ ఇస్తారు.

➢ బాధితుడు అది కూడా నమ్మి మోసగాళ్ళు చెప్పిన ఖాతాలలో డబ్బును డిపాజిట్ చేస్తాడు. కొన్నిసార్లు ఇది లక్షలలో ఉంటుంది.

➢ అయితే బహుమతి మొత్తం ఎంతకూ రాకపోవటంతో తాను లాటరీల పేరుతో మోసపోయినట్లు బాధితుడు కొంతకాలానికి తెలుసుకుంటాడు.

లాటరీ కుంభకోణం : కొన్నిసార్లు "మీరు మిలియన్ డాలర్లు లాటరీలో గెలుచుకున్నారు" అంటూ మీకు ఒక ఇ-మెయిల్ అందుతుంది. ఇలాంటి మెయిల్స్ అందుకోవడం బాగానే ఉంటుంది. అయితే అది నిజమైతేనే బాగుంటుంది. ఇలాంటి మెయిల్స్‌కు స్పందించటం వలన పెద్దమొత్తంలో డబ్బుపోతుంది. మోసగాళ్ళు ఆ డబ్బు ఆశ చూపించి మిమ్ములను బుట్టలో వేసి వదిలేస్తారు.

'మీరు వెబ్‌క్యామ్, డిజిటల్ కెమెరా గెలుచుకున్నారు, అభినందనలు' వంటి ఇ-మెయిల్ కుంభకోణం :

కొన్నిసార్లు మీరు డిజిటల్ కెమెరా లేదా వెబ్ క్యామ్ గెలుచుకున్నారంటూ మీకు ఒక ఇ-మెయిల్ వస్తుంది. దానిని పంపటానికయ్యే ఖర్చులకోసం ఈ క్రింద ఇచ్చిన లింక్‌ను నొక్కి మా వెబ్‌సైట్‌లో మీ క్రెడిట్/ డెబిట్ కార్డు వివరాలు ఇస్తే సరిపోతుందని చెబుతారు. ఆ డబ్బులు మీ ఖాతాలో నుంచి తీసుకోబడతాయిగానీ, మీకు ఆ బహుమతి ఎప్పటికీ అందదు.

ముందు జాగ్రత్త చర్యలు :

➲ ఆన్‌లైన్ లాటరీ లేదా బంపర్ పండుగ బహుమతి అంటూ కొత్తవారి నుంచి ఇ–మెయిల్ గానీ, ఫోన్‌కు ఎస్ఎంఎస్ వస్తే స్పందించకండి.

➲ సరిగ్గా నిర్ధారించుకోకుండా కొత్తవారి ఖాతాలలో డబ్బులు డిపాజిట్ చేయకండి.

➲ తమకు సంబంధంలేని ఒక బ్యాంక్ ఖాతాదారుడికి కమిషన్ ఇచ్చి ఆ ఖాతా నంబర్‌ను వాడుకోవటం ద్వారా మోసగాళ్ళు లాటరీ మోసాలను చేస్తారు.

➲ మోసగాళ్ళు సబ్జెక్ట్‌లైన్‌లో 10,000 డాలర్లు గెలుచుకున్నట్లు ఉండే ఇ–మెయిల్స్ వలలో పడొద్దు. మీ ప్రమేయం లేకుండానే మీకు ఆ మెయిల్ ఎలా వచ్చిందని ఆలోచించండి.

➲ తక్కువ ధరకు వస్తువులు ఇస్తామన్న ప్రకటనలతో అప్రమత్తంగా ఉండండి. మీరు ఆన్‌లైన్ షాపింగ్‌లో గానీ, పోటీలో గానీ పాల్గొనకుండానే మీకు ఆ మెయిల్ ఎందుకు వచ్చిందో ఆలోచించండి.

11. డెస్క్‌టాప్ భద్రత

మీ డెస్క్‌టాప్ కంప్యూటర్‌ను ఎందుకు సురక్షితంగా వుంచుకోవాలి?

మనం పర్సనల్ కంప్యూటర్లను సరైన భద్రతా పరమైన అంశాలు పాటించకుండా వినియోగించడం జరుగుతోంది. చట్ట వ్యతిరేక కార్యక్రమాలకు పాల్పడి వారు ఇలాంటి సురక్షితం కాని కంప్యూటర్లను తమ వనరులుగా మార్చుకోని మోసాలకు పాల్పడుతున్నారు. ఈ మోసాలు వైరస్, ట్రోజాన్స్, కీలాగర్స్ మరియు కొన్ని సమయాలలో నిజమైన హేకర్స్‌గా కూడా ఉండవచ్చు. దీనివల్ల డేటా చోరీకి గురవడం, డేటా పోగొట్టుకోవడం, వ్యక్తిగత సమాచారం బహిర్గతం కావడం, పాస్‌వర్డ్ లాంటి ముఖ్యమైన అంశాలు చోరీకి గురవడం మొదలగునవి జరుగుతున్నవి. కావున మీ పర్సనల్ కంప్యూటర్ భద్రత మరియు రక్షణ విషయంలో ఏమాత్రం రాజీ పడకూడదు.

మార్గదర్శకాలు :

మీ పర్సనల్ కంప్యూటర్ ఉపయోగించే ముందు గుర్తుంచుకోవల్సిన విషయాలు

➲ ఎల్లప్పుడూ లైసెన్సు ఉన్న సాఫ్ట్‌వేర్‌లనే మీ కంప్యూటర్‌లో పెట్టుకోవాలి. దీనివల్ల మీ ఆపరేటింగ్ సిస్టమ్ మరియు అప్లికేషన్స్‌ను ఎప్పటికప్పుడు తాజాగా ఉంచవచ్చు. మీరు ఒకవేళ ఓపెన్ సోర్స్ సాఫ్ట్‌వేర్ వాడుతూవున్నట్లయితే దానిని తరచూ తాజాగా వుంచుకోవడం చేయండి.

➲ డౌన్‌లోడు చేసుకునేటప్పుడు ఎల్లప్పుడూ ఆన్‌లైన్ వెబ్‌సైట్‌లనే వినియోగించండి. అంతేగాని మూడో పార్టీ వారి నుండి డౌన్‌లోడ్ చేయకండి.

➲ డౌన్‌లోడ్ చేసిన ఫైళ్ళను తాజా యాంటి వైరస్ సాఫ్ట్‌వేర్‌తో స్కాన్ చేసిన తర్వాత మాత్రమే ఉపయోగించండి.

➲ ప్రమాదకరమైన వైరస్‌లను నిరోధించడానికి సాఫ్ట్‌వేర్ రక్షణ కవచాన్ని (Firewall) సరిగా అమర్చి ఇన్‌స్టాల్ చేయండి.

బ్రౌజరు భద్రత:



➲ ఎల్లప్పుడూ మీ వెబ్‌బ్రౌజన్‌ను తాజా పాచ్‌లతో అప్‌డేట్ చేసుకుంటూ ఉండండి.

➲ బ్రౌజర్‌లో ఇవ్వబడిన ప్రైవసీ లేదా సెక్యూరిటీ సెట్టింగ్స్ వాడండి.

➲ కంటెంట్ ఫిల్టర్ చేసే సాఫ్ట్‌వేర్‌లను వాడండి.

➲ ఎల్లప్పుడూ సెర్చ్ ఇంజన్ లోని సేఫ్‌సెర్చ్‌ను "ON" లో ఉంచుకోండి.

భౌతిక భద్రత :

➲ మీ కంప్యూటర్ ను దానికి సంబంధించిన భాగాలను తరచూ శుభ్రం చేస్తూ ఉండాలి. సూచన: శుభ్రం చేసేముందు కంప్యూటర్‌ను ఆఫ్ చేయండి.

➲ కంప్యూటర్‌కు సంబంధించిన కరెంటు తీగలు, కేబుళ్ళను నీరు, పురుగులు చేరకుండా సరైన విధంగా అమర్చండి.

➲ పర్సనల్ కంప్యూటర్ పై పనిచేస్తున్నప్పుడు నీరు, ఆహారం అందులో పడకుండా జాగ్రత్తలు తీసుకోండి.

➲ యు.ఎస్.బి. లాంటివి కంప్యూటర్ నుండి తీసివేస్తున్నప్పుడు ఆపరేటింగ్ సిస్టమ్‌లో అందించిన సేఫ్‌లీ రిమూవ్ (Safely Remove) ను ఎంపిక చేసుకుని ఉపయోగించండి.

➲ బయోస్ (BIOS) కు రహస్య సంకేత పదం (పాస్‌వర్డ్) పెట్టుకోవడం ద్వారా ఇతరులు ఎవరూ అక్రమంగా సిస్టమ్‌తో పనిచేయకుండా ఆపవచ్చును.

➲ కంప్యూటర్‌ను వినియోగించని సమయాలలో దానిని ఆఫ్ చేసి ఉంచండి.

సూచన: బయోస్ పాస్‌వర్డ్ ఏర్పాటు చేసుకోవడానికి "Setting password to BIOS" విభాగాన్ని చూడండి.

డేటా భద్రత :

➲ మీ కంప్యూటర్‌లో ఆపరేటింగ్ సిస్టమ్‌ను ఆటో అప్‌డేషన్‌లో ఎనేబుల్ చేసుకుని, క్రమబద్ధంగా అప్‌డేట్ చేస్తూ ఉండాలి.

➲ నమ్మకం ఉన్న వెబ్‌సైట్‌ల నుండి మాత్రమే యాంటీ వైరస్ సాఫ్ట్‌వేర్‌లను డౌన్‌లోడ్ చేసుకొని ఇన్‌స్టాల్ చేసుకోవాలి. కొత్త వైరస్‌ల నిరోధానికి ఎప్పటికప్పుడు దానికదే అప్‌డేట్ అయ్యేలా చూడాలి.

➲ నమ్మకం ఉన్న వెబ్‌సైట్‌ల నుండి మాత్రమే యాంటీ స్పైవేర్‌లను డౌన్‌లోడ్ చేసుకొని ఇన్‌స్టాల్ చేసుకోండి. కొత్త వైరస్‌ల నిరోధానికి ఎప్పటికప్పుడు దానికదే అప్‌డేట్ అయ్యేలా చూడాలి.

➲ విలువైన సమాచారాన్ని భద్రపరచుకోవడానికి ఎన్‌క్రిప్షన్ అనే భద్రతా పరమైన కోడ్ పద్ధతిని వాడండి.

సూచన: దీనికోసం ఎన్‌క్రిప్షన్ పాస్‌వర్డ్ ప్రత్యేకంగా అవసరం. ఎన్‌క్రిప్ట్ చేసినప్పుడు తప్పనిసరిగా పాస్‌వర్డ్‌ను జ్ఞాపకం ఉంచుకోవాలి. లేకపోతే ఆ తర్వాత డేటా అందుబాటులో ఉండదు.

➲ కంప్యూటర్ లోని అడ్మిన్ (Admin) ఖాతాకు సంక్లిష్టమైన పాస్‌వర్డ్ ఇచ్చుకోవాలి. అంతేగాక ఇ-మెయిల్, ఆర్థిక అప్లికేషన్ (అకౌంట్స్) లాంటి ముఖ్యమైన అప్లికేషన్లకు సంక్లిష్టమైన పాస్‌వర్డ్‌ను తప్పనిసరిగా వాడాలి.

➲ బ్యాకప్ (Backup): తరచుగా మీ కంప్యూటర్ లోని డేటాను సి.డి / డి.విడి లేదా యు.ఎస్.బి డ్రైవ్ మొదలైన వాటిలో కాపీ చేసి ఉంచుకోవాలి. ఎందుకంటే మీ కంప్యూటర్ హార్డ్‌డిస్క్ పూర్తిగా దెబ్బతిన్నప్పుడు కాని, రి ఇన్‌స్టాల్ చేస్తున్నప్పుడు కాని లేదా ఫార్మేట్ చేస్తున్నప్పుడు కాని డేటా చెడిపోవచ్చు.

➲ రికవరి డిస్క్ : ధృవీకరించబడని సాఫ్ట్‌వేర్‌లు మరియు ఇతర తెలియని డ్రైవ్‌ల వల్ల బూట్ ఫెయిల్ అయి ఆపరేటింగ్ సిస్టమ్ విఫలమయినప్పుడు, తిరిగి ఆపరేటింగ్ సిస్టమ్ ను రికవరీ చేసుకోవడానికి వీలుగా కంప్యూటర్ తయారీదారుడు లేదా వ్యాపారస్తుడు సరఫరా చేసిన రికవరీ డిస్క్‌ను జాగ్రత్తగా వుంచుకోవాలి.

➲ కంప్యూటర్ స్టార్టర్ ప్రోగ్రాంలను తప్పనిసరిగా పర్యవేక్షణ / నియంత్రణ చేసుకుంటూ తద్వారా సిస్టమ్ పనిచేయు విధానాన్ని మెరుగుపరుచుకోవాలి.

ఇ-మెయిల్ భద్రత :

➲ ఎల్లప్పుడూ మీ ఇ-మెయిల్ ఖాతాకు సంక్లిష్టమైన రహస్య సంకేత పదాన్ని (పాస్‌వర్డ్)ను ఏర్పాటు చేసుకోండి.

➲ వైరస్ స్పామ్‌లు దాడి చేయకుండా నిరోధించేందుకు, ఇ-మెయిల్‌ను స్కాన్ చేసేందుకు గాను ఎల్లప్పుడూ యాంటీ స్పైవేర్ సాఫ్ట్‌వేర్‌ను వినియోగించండి.

➲ ఇ-మెయిల్ అటాచ్‌మెంట్‌లను తెరచే ముందు ఎల్లప్పుడు తప్పనిసరిగా తాజా యాంటీ వైరస్ మరియు యాంటీ స్పైవేర్‌లతో స్కాన్ చేస్తూవుండాలి.

➲ ఎల్లప్పుడూ జ్ఞాపకం వుంచుకొని స్పామ్ ఫోల్డర్ ఖాళీ చేయాలి.

వైర్‌లెస్ భద్రత:

➲ డిఫాల్ట్‌గా ఉన్న అడ్మినిస్ట్రేటివ్ పాస్‌వర్డ్‌లు మార్చుకోవాలి.

➲ డబ్ల్యూ.పి.ఏ (వైై-ఫై ప్రొటెక్టెడ్ యాక్సెస్ / డబ్ల్యూ.ఇ.పి ఎన్‌క్రిప్షన్)ను ఆన్ చేసుకోండి.

➲ డిఫాల్ట్ ఎస్.ఎస్.ఐ.డి. (SSID) ని మార్చండి.

➲ మాక్ (MAC) చిరునామా ఫిల్టర్‌ను ఎనేబుల్ చేయండి

➲ వినియోగించనప్పుడు వైర్‌లెస్ నెట్‌వర్క్‌ను ఆఫ్ చేయండి.

మోడమ్ భద్రత:

➲ డిఫాల్ట్ పాస్‌వర్డ్‌లను మార్చండి

➲ వినియోగించనప్పుడు స్విచ్ ఆఫ్ చేయండి.

(డెస్క్‌టాప్ ఫైర్‌వాల్‌ను ఎల్లప్పుడు ఆన్‌లో ఉంచండి. మీకు తెలుసా 82% మంది గృహ వినియోగదారులకు 2013వ సంవత్సరంలో కనీసం ఒక భద్రతాపరమైన సమస్యనైనా ఎదుర్కొన్నారు)



చేయవలసినవి:

☑ మీరు కంప్యూటరు కొనుగోలు చేసినప్పుడు అమ్మకందారు అందించిన పత్రాలలోని మార్గదర్శకాలను (Guidelines) చదివి పర్సనల్ కంప్యూటర్‌ని ఎలా సెట్ అప్ చేయాలో తెలుసుకోండి

☑ అనుసంధానం చేయండి

- ✓ కీ బోర్డు
- ✓ మౌస్
- ✓ మానిటర్
- ✓ స్పీకర్లు మరియు
- ✓ నెట్‌వర్క్ కేబుల్ లను సి.పి.యుతో అమ్మకందారు ఇచ్చిన పుస్తకంలో సూచించిన విధంగా అనుసంధానం చేయండి.

☑ ఎలక్ట్రికల్ బోర్డులకు మీ సి.పి.యు. మరియు మానిటర్‌ను కనెక్ట్ చేయండి.

చేయకూడనివి :

☒ నకిలీ సాఫ్ట్‌వేర్‌లు ఎలాంటివి అంటే

- ✘ ఆపరేటింగ్ సాఫ్ట్‌వేర్‌లు (Windows, Unix etc.,)
- ✘ అప్లికేషన్ సాఫ్ట్‌వేర్‌లు (Office, Database etc.,)
- ✘ సెక్యూరిటీ సాఫ్ట్‌వేర్‌లను ఇన్‌స్టాల్ చేయకూడదు. సూచన: జ్ఞాపకం వుంచుకోండి. కొన్ని నకిలీ సాఫ్ట్‌వేర్‌లు వాటికవే మోసపు ప్రోగ్రాములు.

☒ మీ కంప్యూటర్‌ను నేరుగా ఎలక్ట్రికల్ ప్లగ్ పాయింట్‌కు కనెక్ట్ చేయకండి. అనుకోకుండా వచ్చే ఎక్కువ కరెంటు (హై వోల్టేజి) ప్రవాహం వల్ల కంప్యూటర్ దెబ్బతినవచ్చు. దానికి బదులుగా నమ్మకమైన ఒక సర్జ్ ప్రొటక్టర్ ద్వారా కంప్యూటర్‌ను కలపండి.

☒ మీరు కంప్యూటర్ చుట్టుప్రక్కల ఆహారం తినడం లేదా తాగడం చేయకండి.

☒ కంప్యూటర్‌కు దగ్గరగా అయస్కాంతాలను ఉంచకండి.

☒ కంప్యూటర్ పరికరములపై ఎలాంటి ద్రవాలను చల్లకండి. ఒకవేళ అలా చేయవలసిన అవసరం ఉందనుకుంటే ముందుగా ఒక బట్టపైన స్ప్రే చేసి ఆ బట్టతో ఈ పరికరములను తుడవండి.

☒ రెండు ఎక్స్‌టెన్షన్స్ ఉన్న ఇ-మెయిల్ అటాచ్‌మెంట్‌లను తెరవకండి.

వైర్‌లెస్ మోడమ్‌ను కనెక్ట్ చేసేముందు పాటించవలసిన సూచనలు :

➲ మీరు కనెక్ట్ చేసే ముందు మీ వైర్‌లెస్ మోడమ్ ప్యాకేజీలో మీకు తగిన పరికరములు అందుబాటులో ఉన్నాయా లేవా నిర్ధారించుకోవాలి. వైర్‌లెస్ మోడమ్ (లేదా వైర్‌లెస్ అడాప్టర్), ఇన్‌స్టాలేషన్ సి.డి. ర్యామ్‌తో పాటు మాన్యువల్, ఈతర్నెట్ కేబుల్ (లేదా యు.ఎస్.బి. కేబుల్ – మీకు వైర్‌లెస్ మోడమ్ అయితే), ఒక వైర్‌లెస్ యాంటీనా (802.11a, 802.11b or 802.11g) అనే వైర్‌లెస్ ప్రమాణాలు ఉన్నాయా లేవా నిర్ధారించుకోవాలి మరియు కరెంటు అడాప్టర్ ఉండాలి. ఇందులో ఏదైనా లేకపోతే వైర్‌లెస్ మోడమ్ కొన్న షాపువారిని లేదా ఉత్పత్తిదారుడికి ఫోన్ చేసి పిలవాలి.

➲ మాన్యువల్‌ను పూర్తిగా చదివి పరికరములు ఎలా పనిచేస్తాయో తెలుసుకోవాలి. ఉదాహరణకు వైర్‌లెస్ యాంటీనా, వైర్‌లెస్ నెట్ వర్క్‌కు కనెక్ట్ చేసినప్పుడు, ఈతర్నెట్ కేబుల్‌ను (యు.ఎస్.బి కేబుల్) కంప్యూటర్ మోడమ్‌కు కనెక్ట్ చేసినప్పుడు ఎలా పనిచేస్తుందో తెలుసుకోవాలి.

➲ మీ వైర్‌లెస్ యాంటీనాను మోడమ్‌కు జతచేయాలి.

➲ ఈతర్నెట్ కేబుల్‌ను మీ కంప్యూటర్‌లోని లాన్ లేదా ఈతర్నెట్ పోర్టు మోడమ్‌కు తగిలించాలి. లేదా మీకు ఒకవేళ వైర్‌లెస్ యు.ఎస్.బి మోడమ్ ఉంటే యు.ఎస్.బి కేబుల్‌ను యు.ఎస్.బి పోర్టులో పెట్టాలి.

➲ విద్యుత్ బోర్డుకు మోడమ్ విద్యుత్ అడాప్టర్‌ను కనెక్ట్‌చేయాలి. ఫ్లగ్ లోనికి పెట్టి స్విచ్ ఆన్‌చేయాలి.

వైర్‌లెస్ మోడమ్‌ను ఏర్పాటు చేసుకోవడం:

➲ మీ వెబ్ బ్రౌజరును తెరచి అందులో మోడమ్‌కు చెందిన అడ్మినిస్ట్రేటివ్ వెబ్‌సైట్ URL ను ఎంటర్ చేయాలి. వినియోగదారుల మాన్యువల్ లేకపోతే మీరు మెడమ్ ఉత్పత్తిదారులకు లేదా డీలరు వారి కస్టమర్ సర్వీసుకు ఫంక్షన్ చేయవచ్చును.

➲ యూజర్ మాన్యువల్‌లో ఇచ్చినట్టు అడ్మినిస్ట్రేటివ్ వెబ్‌సైట్‌లోకి తెరిచాక యూజర్ మాన్యువల్‌లో ఇచ్చిన మేరకు అందులో యూజర్ నేమ్, పాస్‌వర్డ్ ఎంటర్ చేయాలి. ఒకవేళ మీరు దీనిని తెలుసుకోలేక పోతే మీరు మోడమ్ ఉత్పత్తిదారులకు లేదా డీలరు వారి కస్టమర్ సర్వీసుకు ఫోన్ చేయవచ్చును. సాధారణంగా డీఫాల్ట్‌గా ఉండే యూజర్ నేమ్ “Admin” గా ఉంటుంది.

➲ ఇంటర్నెట్ రకమేదో సెలక్టు చేసుకోవాలి. ఇంటర్నెట్ కనెక్షన్‌లో నాలుగు రకాల కనెక్షన్లు ఉంటాయి. “Dynamic IP Address”, “Static IP Address”, “PPPoE/ PPPoA”

and "Bridge Mode" అనేవిగా ఉంటాయి. మీ ఇంటర్నెట్ సర్వీసు అందించే సంస్థవారికి ఫోన్ చేసి ఏ సెట్టింగు మీకు సరిగ్గా సరిపోతుందో తెలుసుకోవాలి.

➲ ఐ.ఎస్.పి సర్వర్ నుండి మీరు ఆటోమేటిక్‌గా ఐ.పి. అడ్రసు తీసుకోవాలంటే "Dynamic IP Address" ఎంపిక చేసుకోవాలి. మీరు తీసుకునే ప్రతి వైర్‌లెస్ కనెక్షన్‌కు మీకు ఒక ఐ.పి. అడ్రసు వస్తుంది. కొన్ని సందర్భాల్లో ఐ.పి. అడ్రసు మారుతూ ఉంటుంది. (మీరు ఇంటర్నెట్ కనెక్టయిన ప్రతిసారీ మీ ఐ.పీ. మారుతూ ఉంటుంది) మరియు ఇతర సందర్భాల్లో ఎలాంటి మార్పు లేకుండా స్థిరంగా ఉంటుంది. (మీరు ఇంటర్నెట్ కనెక్టయినా, డిస్‌కనెక్టయినా ఒకే ఐ.పి. అడ్రసు స్థిరంగా ఉంటుంది. అడ్రసు మారుతూ ఉంటే మీరు ఈ సెట్టింగును ఎంపిక చేసుకుంటే మంచిది. ఎప్పుడయితే వైర్‌లెస్ అవుతుందో మోడమ్ కూడా ఆటోమేటిక్‌గా మారుతూ సర్వర్ నుండి కొత్త ఐ.పి. అడ్రసు తీసుకుంటూ ఉంటుంది. మీ మాక్ అడ్రసు ఎంటర్ చేసి (MAC Address) (సాధారణంగా ఇది మోడమ్‌కు వెనుక భాగమున ఉంటుంది.) ఇతర వివరములు ఎంటర్ చేయాలి. యూజర్ మాన్యువల్‌ను పరిశీలించడం లేదా మోడమ్ ఉత్పత్తిదారుని యొక్క / షాపువారి యొక్క కస్టమర్ కేర్ సెంటర్ నుండి ఇతర వివరములు తీసుకోవాలి.

➲ "Static IP Addrsee" ను ఎంపిక చేసుకొని స్థిరమైన ఐ.పి. అడ్రసు పొందవచ్చు. మీరు "VPI", "VCI", "IP Address", "Subnet Mask", "ISP Gateway Address", "Server Address", "Primary DNS Address", "Secondary DSN Address" మరియు "Connection Type" అనేవి పూర్తిచేయవలసి ఉంటుంది. ఈ వివరములు మీరు సర్వీస్ ప్రొవైడరు నుండి తీసుకోవాలి.

➲ "PPPoE/ PPPoA" ఈ రకమైన ఐ.ఎస్.పి వినియోగదారుడై ఉంటే DSL వినియోగదారులు ఈ కనెక్షన్ వినియోగించవచ్చు. మీ యూజర్ నేమ్, పాస్‌వర్డ్ మరియు ఇతర వివరములు ఎంటర్ చేయవలసి ఉంటుంది. ఇవన్నీ సర్వీస్ ప్రొవైడర్స్ అందిస్తారు.

➲ "Bridge Mode" అనే రకం ఎంపికదారులైతే మీరు ఐ.ఎస్.పి లో ఈ రకమైన దానిని ఎంపిక చేసుకోవాలి. సర్వీసు ప్రొవైడర్ అందించిన సంబంధించిన వివరములను ఎంటర్ చేయాలి.

➲ మీ పని పూర్తయిన తరువాత "Finish" or "OK" అనే దానిపై క్లిక్ చేయవలసి ఉంటుంది. ఇప్పుడు మీ మోడమ్ సెటప్ పూర్తయినట్టే.

➲ ఇంటర్నెట్ వస్తున్నదా లేదా అని తెలుసుకోవడానికి మీ బ్రౌజర్ నందు యు.ఆర్.యల్ అడ్రసు ఎంటర్ చేయండి.

వైర్లెస్ నెట్వర్క్స్ వాడినప్పుడు డెస్క్‌టాప్ ఫైర్వాల్‌ని ఉపయోగించండి

సెటప్స్ : బయాస్ సెట్టింగ్స్ (Basic Input / Output System)

➲ కంప్యూటర్ బయాస్ అనేది కంప్యూటర్‌ను ఆన్ చేయగానే మొదటగా పనిచేసే ప్రోగ్రాం. ఎప్పుడయితే మీరు కంప్యూటర్ స్టార్ట్ చేస్తారో అప్పుడు పాస్‌వర్డ్ అడుగమని బయాస్‌కి చెప్పవచ్చు. దీనివల్ల కంప్యూటర్‌ను ఇతరులు పనిచేయకుండా నియంత్రించవచ్చు.

➲ బయాస్ సెటప్ ప్రోగ్రాంలోకి ఎంటర్ అవడానికి, కొన్నిసార్లు దీనిని సి.యం.ఓ.ఎస్ సెటప్ అని అంటారు. మీ కంప్యూటర్‌ను ఆరంభించండి లేదా రీబూట్ చేయండి. కంప్యూటర్ స్క్రీన్ పై పలు రకాల డయాగ్నొస్టిక్స్ మరియు మెమరి చెక్‌లను డిస్‌ప్లే చేస్తుంది. ఆ సమయంలో "Hit the <DEL> key to enter the BIOS setup program" అనే సమాచారం కనిపిస్తుంది. ప్రతిసారి DEL కీ కాకపోవచ్చు. కొన్ని బయాస్‌లు F2 లేదా F10 లేదా ఇతర కీలతో కలిపిన వాటిని ఉపయోగించుకోవచ్చు. వీటికోసం మీ మదర్ వాటిని ఉపయోగించు కోవచ్చు. వీటికోసం మీ మదర్ బోర్డు మాన్యువల్‌ను ఇంకా ఎక్కువ వివరాలకోసం చూడండి.

సూచన : కొన్ని బయాస్‌లు గ్రాఫికల్ రకం ఐకాన్‌లు గల మెను (a GUI) లేదా పదాలు ఒక దానితో ఒకటి కలిసి ఏర్పడేటట్లు, ఏ రకమైనా దాని సూత్రంలో మాత్రం సరిగ్గా అదే ఉంటుంది.

➲ పాస్‌వర్డ్‌కు సంబంధించి రెండు రకాల ప్రత్యామ్నాయాలు ఉన్నాయి. సూపర్‌వైజర్ పాస్‌వర్డ్ మరియు యూజర్ పాస్‌వర్డ్. ఇవి బయాస్ సెటప్ ప్రోగ్రామును నియంత్రించేందుకు మరియు కంప్యూటర్ బూట్‌కు సంబంధించినదిగాను ఉంటాయి.

సూచన : అన్ని బయోస్‌కు ఈ పాస్‌వర్డ్‌లు ఉండకపోవచ్చు. మీ బయోస్‌కు ఈ అవకాశం లేకపోతే మీరు ఈ విషయంలో మీ కంప్యూటర్ ఉపయోగించడంలో ఇతరుల ప్రమేయాన్ని నియంత్రించ లేదు.

➲ మీరు యూజర్ పాస్‌వర్డ్ ఎంపిక చేసుకుంటే మీరు సరైన పాస్‌వర్డ్‌ను తప్పనిసరిగా ఎంటర్ చేయాలి. మీరు ఎనిమిది అక్షరాలు కలిగిన పాస్‌వర్డ్‌ను ఎంటర్ చేయాలి (ఎక్కువ బయోస్‌లలో దురదృష్టవశాత్తు ఎనిమిది అక్షరాలకే దీనిని పరిమితం చేయడం జరిగింది) నేను చెప్పేది ఏమిటంటే మీరు ఎనిమిది అక్షరాల నిడివి కలిగిన పూర్తి పాస్‌వర్డ్‌ను ఉపయోగించండి. అయితే అది మీరు మరచిపోయేదిగా ఉండరాదు. అనంతరం బయోస్ మీ పాస్‌వర్డ్‌ను నిర్ధారిస్తుంది. మీరు వెంటనే అదే టైప్ చేస్తే చాలు. ఇప్పుడు మీ సిస్టమ్ ప్రతిసారీ బూట్ అయ్యేటప్పుడు లేదా మీరు ప్రారంభించినప్పుడు ఈ పాస్‌వర్డ్ చెక్ ఆప్షన్ మీకు దీనిపై ఆసక్తి ఉంటే మీరు ఎంపికచేసుకొని ALWAYS ను సెటింగు మార్చుకోవాలి.

మీరు మళ్లీ వెనక్కు వచ్చి ప్రధాన మెనులో సేవ్ & ఎగ్జిట్ సెటప్ (SAVE & EXIT SETUP) ను సెలక్టు చేసుకోవాలి. ఇప్పుడు మీ కంప్యూటర్ రీబూట్ అవుతుంది మరియు మిమ్మల్ని పాస్‌వర్డ్ కొరకు అడుగుతుంది. ప్రతిసారీ మీరు బూట్ చేసినప్పుడు పాస్‌వర్డ్‌ను అడుగుతుంది.

సూచన : ఈ పద్ధతి కేవలం మీ కంప్యూటర్ లోనికి ప్రవేశించేందుకు మాత్రమే కాని పూర్తి భద్రతకు సంబంధించినవి కాదు. దీనికి ఇంకా పలు మార్గాలు ఉన్నాయి. అయితే ఇది ఎక్కువ మొత్తంలో సమస్యలు రాకుండా కొంతవరకు నిరోధించగలుగుతుంది.

సూచన : మీరు ఒకవేళ బయోస్ పాస్‌వర్డ్‌ను మరచిపోతే మీ కంప్యూటర్ మదర్ బోర్డు మాన్యువల్‌ను సంప్రదించవచ్చు. అది మీ దగ్గర లేకపోతే బయోస్ వెబ్‌సైట్‌లో బయోస్ ఉత్పత్తిదారుడిని సంప్రదించవలసి వుంటుంది.

12. మొబైల్ ఫోన్ భద్రత

మొబైల్ ఫోన్ అనేది ఎన్నడూ లేనంతగా ప్రస్తుతం చాలా ప్రాచుర్యంలోనికి వచ్చేసింది. అంతేగాక వివిధ రకాల వేగవంతమైన సౌకర్యాలతో వినియోగదారుని ఆకర్షిస్తూ అపకారం కూడా కలగజేస్తోంది.

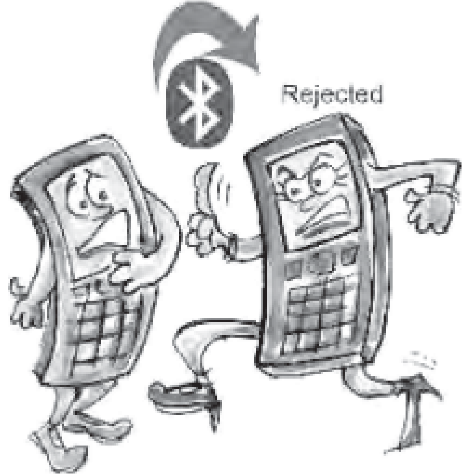
సాంప్రదాయ డెస్క్‌టాప్ కంప్యూటర్లకు లాగానే మొబైల్ ఫోన్లకు కూడా భద్రత సవాళ్ళు ఎదురవుతున్నాయి. అయితే కంప్యూటర్ లా దీనిని ఒక దగ్గరే పెట్టకుండా మనతో పాటు తీసుకెళుతున్నామంటేనే కొంత ప్రమాదానికి గురయ్యే అవకాశం ఉన్నట్టే కదా.

మొబైల్ ఫోన్‌లు కూడా వైరస్‌ల బారిన పడుతున్నాయి. ట్రోజన్ హార్స్ అనే వైరస్ లేదా ఇతర వైరస్ జాతికి చెందిన వైరస్‌ల భారిన పడుతున్నాయి. ఇవి మీ మొబైల్ ఫోన్ రక్షణ విషయంలో రాజీ పడాల్సి వస్తుంది. అంతేగాకుండా వ్యక్తిగత సమాచారం మరియు మొబైల్ పైన పూర్తి నియంత్రణ సాధించి దెబ్బతీస్తాయి.

ఈ మార్గదర్శి మొబైల్ వాడకంలో అవసరమైన మార్గాలు, చేయదగిన, చేయకూడని అంశాలు మరియు మొబైల్ ఫోన్ భద్రతకు ఉపకరించే సూచనలను అందిస్తుంది.

మొబైల్ ఫోన్ వినియోగించే ముందు పాటించవలసిన అంశాలు :

అంశం 1 : మొబైల్ ఫోన్ ఉత్పత్తి సంస్థలు అందజేసిన తమ ఉత్పత్తుల వివరాలతో కూడిన పుస్తకములోని అంశాలను జాగ్రత్తగా చదవాలి. మొబైల్ ఫోన్ వినియోగానికి మరియు సెట్ అప్ నకు సంబంధించి అందులో పొందుపరచిన మార్గదర్శక విషయాలను పాటించాలి.



అంశం 2 : మొబైల్ ఫోన్‌కు చెందిన ఐ.యం.ఇ.ఐ (IMEI - International Mobile Equipment Identity) నెంబరును ఎక్కడైనా వ్రాసి ఉంచు కోవాలి.

ఎందుకంటే ఎప్పుడైనా మొబైల్ ఫోన్‌ను పోగొట్టుకుంటే దాని జాడను తెలుసుకునేందుకు ఇది ఉపయోగపడుతుంది.

సూచన : సాధారణంగా ఈ ఐ.యం.ఇ.ఐ సంఖ్య ఫోన్ లోని బ్యాటరీకి క్రింది భాగంలో ముద్రించి ఉంచుతారు. లేదా చాలా ఫోన్లలో ***#06#** అనే సంకేతాన్ని డయల్ చేసి కూడా మీరు ఐ.యం.ఇ.ఐ సంఖ్యను తెలుసుకోవచ్చును.

➢ ఇంకా విస్తృత సమాచారానికి ఉత్పత్తిదారుడు ప్రచురించిన సమాచార పుస్తకంలో చూడండి.

మొబైల్ ఫోన్ సంరక్షణ విషయంలో భయపెట్టే రకాలు :

➢ మొబైల్ పరికరం మరియు అందులోని సమాచారం (డేటా) రక్షణ భయాలు

✡ అనధికారికంగా లేదా ప్రణాళికాబద్ధంగా మొబైల్ పరికరానికి అందుబాటు లేదా పోగొట్టుకోవడమో లేదా దొంగతనానికి గురిఅవడం అనే భయాలు వున్నాయి.

➢ మొబైల్‌కు అనుసంధానం విషయంలో రక్షణా భయాలు

✡ మొబైల్ ఫోన్ అనుసంధానం (కనెక్షన్) విషయంలో భయపడే అంశాలు అంటే ముఖ్యంగా ఫోన్‌లలో నింపిన ప్రోగ్రాంలు వాటి నెట్‌వర్క్‌లు తెలియకపోవడం మరియు బ్లూటూత్, వైఫై, యు.ఎస్.బి. వంటి సాంకేతిక అంశాలను వాడడం పట్ల సరైన అవగాహన లేకపోవడం జరుగుతోంది.

➢ మొబైల్‌లో ఉన్న విషయాలను వాడడం మరియు ఆపరేటింగ్ సిస్టమ్‌ల రక్షణ భయాలు

✡ మొబైల్ ఫోన్ ఆపరేటింగ్ సిస్టమ్ మరియు అప్లికేషన్స్ వాడే విషయంలో తరచూ ఇబ్బందులు ఎదురుకావడం.

మొబైల్ ఫోన్ ద్వారా ఎదుర్కొనే వివిధ రకాల సమస్యల ప్రభావాలు :

➲ మొబైల్ ఫోన్‌లో ఉన్న వినియోగదారుడి వ్యక్తిగత సమాచారం లేదా డేటా పోగొట్టుకోవడం, బహిర్గతమవ్వడం.

➲ వివిధరకాల తెలియని చెడును చేయు నిర్వహణా పద్ధతి (Software)ని వినియోగించడం వల్ల ఉన్నతశ్రేణి మరియు ఖరీదైన సంక్షిప్త సమాచారం (SMS) మరియు ఫక్షన్‌లో సంభాషించు (Call Services) సేవల వల్ల ఆర్థికంగా నష్టం జరుగుతుంది.

➲ వినియోగదారుడికి తెలియకుండానే అతని వ్యక్తిగత స్వేచ్ఛను హరించే అంశాలను తెలుసుకోవచ్చు. ముఖ్యంగా అతని మొబైల్ ఫోన్ ఏ ప్రాంతంలో ఉన్నదో కూడా జాడ వెతికి పట్టవచ్చు. ప్రైవేట్ చిన్న సంక్షిప్త సమాచారం ఇవ్వడం, వినియోగదారునికి తెలియకుండా కాల్స్ చేయడం కూడా చేయవచ్చు.

➲ మొబైల్ ఫోన్‌పై నియంత్రణ కోల్పోవడమే కాకుండా తెలియకుండానే యాంత్రికంగా దాని ప్రభావానికి గురవుతాము.

మొబైల్ ఫోన్ మరియు సమాచారం భద్రత అంశాలపై ఎదురయ్యే సమస్యలను తగ్గించడానికి సూత్రాలు

చేయవలసినవి :

☑ ఐ.యం.ఇ.ఐ (IMEI) సంఖ్యను వ్రాసి ఉంచుకోవడం మొబైల్ ఫోన్‌కు చెందిన 15 అంకెల ఐ.యం.ఇ.ఐ (IMEI - International Mobile Equipment Identity) నెంబరును ఎక్కడైనా వ్రాసి ఉంచుకోవాలి. ఎందుకంటే ఎప్పుడైనా మొబైల్ ఫోన్‌ను

పోగొట్టుకుంటే పోలీసు స్టేషన్‌లో ఫిర్యాదు చేయాలంటే ఇది తప్పనిసరి. దాని జాడను తెలుసుకునేందుకు సేవలు అందించే సంస్థల ద్వారా కనుగొనే వీలవుతుంది.

☑ మొబైల్ పరికరం లాక్ చేయడం.

మీ మొబైల్ ఫోన్ లోని సమాచారాన్ని వేరే వారు తీసుకోకుండా నియంత్రించేందుకు గాను రహస్య సంకేతం ఉపయోగించి దానికదే లాక్ అయ్యే విధమైన పద్ధతిని వినియోగించాలి.

☑ వ్యక్తిగత గుర్తింపు సంఖ్య వాడటం ద్వారా సిమ్‌కార్డును చోరీకి గురయిన సందర్భంలో కూడా దుర్వినియోగం కాకుండా భద్రంగా ఉంచుకోవచ్చు. సిమ్ భద్రతా అంశానికి వస్తే మొబైల్ ఫోన్ వాడడం మొదలు పెట్టిన ప్రతిసారి సిమ్ రహస్య సంకేతం (PIN) ద్వారానే ప్రవేశించే పద్ధతిని అవలంభించడం శ్రేయస్కరం.

మెమోరీ కార్డులోని సమాచారం భద్రంగా ఉండాలంటే రహస్య సంకేత పదాన్ని వాడాలి.

☑ చోరీకి గురైన మొబైల్ ఫోన్‌కై ఫిర్యాదు చేయడం.

మొబైల్ ఫోన్ పోగొట్టుకున్నప్పుడు లేదా చోరీకి గురయితే వెంటనే సమీపంలోని పోలీసు స్టేషన్‌లో ఫిర్యాదు చేయాలి మరియు సేవలు అందించు సంస్థలకు సమాచారం ఇవ్వాలి. ఫోన్ జాడను తెలుసుకునే పద్ధతిని అవలంభించాలి.

ఫోన్ పోగొట్టుకున్నా లేదా చోరీకి గురైన తరువాత జాడను తెలుసుకునే పద్ధతిని వినియోగించితే అది సహాయకారిగా ఉపయోగపడుతుంది. ప్రతిసారీ కొత్త సిమ్ కార్డు మొబైల్ ఫోన్‌లో వేసినప్పుడు మీరు ముందుగానే మీ ఇష్టం మేరకు ఎంపిక చేసుకున్న ఫోన్ నెంబర్లకు సమాచారం దానికదే అందిస్తుంది. దీంతో మొబైల్ ఫోన్ ఎక్కడ ఉందనే జాడను సులభంగా గుర్తించవచ్చు.

చేయకూడనివి :

☒ ఎప్పుడూ మీ ఫోన్ ను అందుబాటలో లేకుండా వదలి పెట్టకండి.

☒ వినియోగించనప్పుడు ఫోన్ లోని కెమెరా, ఆడియో, వీడియోవ లాంటి అప్లికేషన్లు మరియు బ్లూటూత్, ఇన్‌ఫ్రారెడ్, వై –ఫై లాంటి కనెక్షన్లను ఆఫ్‌లో ఉంచాలి. కనెక్షన్లు అలాగే ఆన్‌లో ఉంచితే భద్రతాపరమైన సమస్యలతో పాటు బ్యాటరీ ఛార్జింగ్ త్వరగా అయిపోతుంది.

డేటా భద్రతా విషయంలో చేయదగినవి :

➢ **నిరంతరం డేటా బ్యాకప్ చేయడం**

మొబైల్ లోని సెటప్‌లో సమాచారం మార్పుచేర్పులకు గురైనప్పుడు దాని బ్యాకప్ నిరంతరం జరిగే విధంగా పద్ధతిని ఎంపిక చేసుకోవాలి. అంతేగాక మొబైల్ లోని సమాచారాన్ని వేరొక ప్రత్యేక మెమరికార్డులో కూడా సేవ్ చేసి ఉంచుకోవాలి. వెండర్స్ డాక్యుమెంట్ బ్యాక్ అప్ పద్ధతి (Vendor’s document backup procedure) ని వాడడం ద్వారా ఈ సౌకర్యం పొందవచ్చు.

➢ కర్మాగారం ఏర్పాటు చేసిన సెట్టింగ్‌ల స్థానంలో తిరిగి కొత్తగా ఏర్పాట్లు చేసుకోవడం

➢ మీ మొబైల్ ఫోన్‌ను శాశ్వతంగా వేరొకరికి ఇచ్చి వేస్తున్నప్పుడు తప్పనిసరిగా కర్మాగారంలో మొబైల్ ఫోన్‌లో ఏర్పాటు చేసిన వ్యవస్థలను తిరిగి కొత్తగా ఏర్పాటు చేసి ఇవ్వాలి. అందులోని మీ వ్యక్తిగత సమాచారం మరియు డేటాను చెరిపివేయాలి.

మొబైల్ ఫోన్ కనెక్షన్ అనుసంధాన భద్రతపై ఎదురయ్యే సమస్యలను తగ్గించడానికి సూత్రాలు

➢ **బ్లూటూత్:** బ్లూటూత్ అనేది ఎలాంటి తీగలు లేని అనుసంధాన సాంకేతిక పరిజ్ఞానం ఈ ప్రక్రియ ద్వారా ఒక మొబైల్ ఫోన్ లోను సమాచారాన్ని మరియు డేటాను వేరొక మొబైల్ ఫోన్‌కు అనుసంధానం చేసి ఇచ్చి, తీసుకోవడానికి ఉపయోగిస్తారు. దీని ద్వారా ఫోటోలు, రింగ్‌టోన్స్‌ను మార్పిడీ చేసుకొనవచ్చును. ఈ తీగలు లేని బ్లూటూత్ దాదాపు 30 అడుగుల (10 మీటర్లు) వరకు సిగ్నల్స్ పంపుతుంది.

చేయదగినవి :

☑ బ్లూటూత్‌ను కనబడని రీతిలో (హిడన్ మోడ్‌లో) వినియోగించాలి. దీనివల్ల ఇతరులకు మీరు బ్లూటూత్ వాడుతున్న విషయం తెలియదు.

☑ మొబైల్ పరికరం పేరును ఇతరులు గుర్తించకుండా మొబైల్ ఫోన్ రకము మార్చివాడాలి.

సూచన : బ్లూటూత్ పరికరములకు మొబైల్ రకపు నెంబరుకుండే నిర్ధేశిత పేరు.

☑ ఇంకొకరి మొబైల్ ఫోన్‌తో జతకడుతున్నప్పుడు పాస్‌వర్డ్ ఇవ్వాలి. ఇదే పాస్‌వర్డ్‌తో మీ కంప్యూటర్ కనెక్ట్ అవుతుంది.

☑ సమాచారాన్ని ప్రసారం చేయని సందర్భాలలో బ్లూటూత్‌ను ఆపి ఉంచాలి.

☑ బ్లూటూత్ తాత్కాలికంగా కొంత సమయం వరకే వినియోగించి దానికదే బ్లూటూత్ ఆగిపోయేవిధంగా పెట్టుకోవాలి. దీనివల్ల మిగిలిన వాళ్ళకు మీ బ్లూటూత్ ఎల్లప్పుడూ అందుబాటులో ఉండదు.

చేయకూడనివి :

☒ మీకు తెలియని మొబైల్ పరికరములతో బ్లూటూత్ ద్వారా ఎప్పుడూ అనుసంధానంను అంగీకరించకండి.

☒ బ్లూటూత్‌ను నిరంతరంగా చురుకుగా ఆన్‌లోనే ఉంచకండి.

☒ ఇతరులకు కనిపించే విధంగా బ్లూటూత్‌ను ఎల్లప్పుడూ పెట్టకండి.

సూచన : బ్లూటూత్ ఎల్లప్పుడూ డీఫాల్ట్‌గా ఆన్‌లోనే ఉంచితే సమస్యలు ఎదురవుతాయి. సమస్యలు సృష్టించే వారికి అది అవకాశంగా మారుతుంది. ఎల్లప్పుడూ కనిపించని విధంగా సెటింగ్ ఏర్పాటు చేసుకుంటే సమస్యలు రాకుండా ఉంటుంది.

వై-ఫై: వై–ఫై అనేది తీగలు లేని విశ్వసనీయముగా పనిచేయు అనే పదానికి సంక్షిప్త రూపం. వై–ఫై అనేది తీగలు లేని నెట్‌వర్క్ సాంకేతిక పరిజ్ఞానం. ఇది కంప్యూటర్లు మరియు ఇతర పరికరములు ద్వారా తీగలు లేని సిగ్నల్స్‌ను ప్రసారం చేస్తుంది. పలు మొబైల్ ఫోన్‌లలో వీడియో గేమ్‌ల పద్ధతి ఉంటుంది. మరియు ఇతర ప్రత్యేకత కలిగిన పరికరములు కూడా వై–ఫై సామర్థ్యం కలిగి తీగలు లేని వ్యవస్థకు అనుసంధానం అవుతుంది. ఈ పరికరములు అంతర్జాలంకు అనుసంధానం చేయగలుగుతాయి.

చేయదగినవి :

☑ నమ్మకమైన నెట్‌వర్క్ వ్యవస్థలకే అనుసంధానమవ్వాలి.

☑ అవసరమైనప్పుడు మాత్రమే వై–ఫై వాడాలి. దీనిని వాడనప్పుడు ఆపి ఉంచడం అనేది సూచించడమైనది.

☑ ప్రజా అనుసంధాన నెట్‌వర్క్‌లతో పని చేసేటప్పుడు జాగ్రత్తగా ఉండాలి. అవి సురక్షితమైనవి కావు.

చేయకూడనివి :

☒ తెలియని మరియు నమ్మకం లేని నెట్‌వర్క్‌లకు ఎప్పుడూ అనుసంధానం కాకూడదు.

మొబైల్‌ను యు.ఎస్.బి గా వాడడం :

కంప్యూటర్‌కు అనుసంధానం చేయడం ద్వారా మొబైల్ ఫోన్లను యు.ఎస్.బి మెమరీ పరికరముగా కూడా వినియోగించవచ్చు. యు.ఎస్.బి. కేబుల్ ప్రత్యేకంగా మొబైల్ ఫోన్‌ను కంప్యూటర్‌కు కనెక్ట్ చేయడానికి ఉపయోగిస్తారు. మీ మొబైల్ ఫోన్ మెమరీ మరియు మెమరీ కార్డు యు.ఎస్.బి లా పనిచేస్తాయి.

చేయదగినవి :

☑ పర్సనల్ కంప్యూటరుకు మొబైల్ ఫోన్‌ను కనెక్ట్ చేసినప్పుడు ఫోన్ మెమరీ కార్డును మరియు మెమరీ కార్డును తాజా వైరస్ నిరోధకంతో స్కాన్ చేయాలి.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

Chittoor Police 9440900005

13. ఫిషింగ్ దాడులు

ఫిషింగ్ అనేది సమాచారాన్ని మోసపూరితంగా సేకరించే ఒక పద్ధతి. ఇందులో యూజర్‌నేమ్, పాస్‌వర్డ్, పిన్ నెంబరు, బ్యాంకు ఖాతా, క్రెడిట్ కార్డు వివరములు బాగా నమ్మకం ఉన్న సంస్థలా ముసుగేసుకొని మనకు తెలియకుండానే రకరకాలుగా ఇ-మెయిల్, ఫోన్ లాంటి వాటి ద్వారా సమాచారాన్ని సేకరిస్తారు.



ఫిషింగ్ సాధారణంగా ఇ-మెయిల్‌ను పంపడం ద్వారా లేదా సంక్షిప్త సమాచారం ద్వారా చేస్తారు.

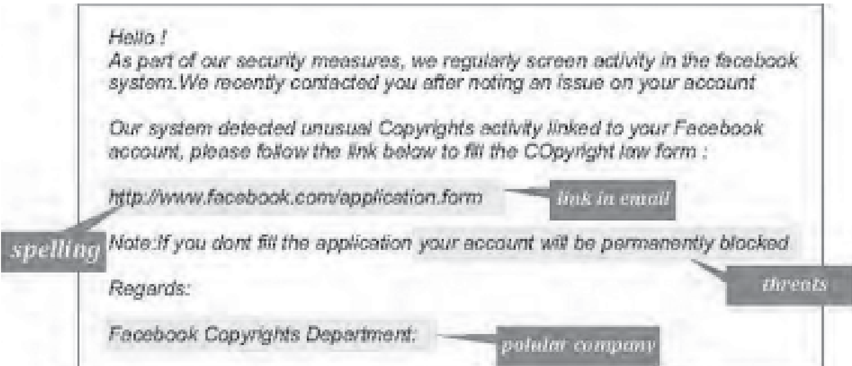
నకిలీ వెబ్‌సైట్‌లు చట్టబద్ధత కలిగి ఉన్నట్టుగా తయారుచేసి వివిధ రూపాలలో ఆకర్షిస్తారు.

దీంతో వినియోగదారుడే తమ వివరాలు అందించి మోసానికి గురయ్యే అవకాశం ఉన్నది.

వినియోగదారుడిని నమ్మించి మోసం చేసే సామాజిక ఇంజనీరింగ్ పద్ధతిని ఫిషింగ్‌కు ఒక ఉదాహరణగా చెప్పుకోవచ్చు.

ఫోన్ ద్వారా కూడా ఫిషింగ్ చేయవచ్చు. అందుకని ఫోన్‌లో మీ వ్యక్తిగత సమాచారం ఎవ్వరికీ అందించకండి.

ఫిషింగ్ ఇ-మెయిల్‌లో సమాచారం ఎలా కన్పిస్తూ వుంటుంది? వివరంగా చూద్దాం ....



Hello !
As part of our security measures, we regularly screen activity in the facebook system.We recently contacted you after noting an issue on your account

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the COpyright law form :

http://www.facebook.com/application.form

Note:If you dont fill the application your account will be permanently blocked

Regards:

Facebook Copyrights Department:

➢ **స్పెల్లింగ్ మరియు గ్రామరు తప్పులు**

లింక్‌లు మిమ్మల్ని .exe ఫైళ్ళకు తీసుకువెళ్ళవచ్చు.

ఈ రకమైన ఫైళ్ళు వైరస్‌ను వ్యాపించి నష్టం చేసేవిగా ఉంటాయి.

➢ **భయాలు**

కొన్నిసార్లు మీకు హెచ్చరిక ఇ–మెయిల్ వస్తుంది.

ఇ–మెయిల్‌కు మీరు స్పందించి మీ వెబ్ మెయిల్ ఖాతా వివరములు పంపకుంటే అది ఇకపై మూసివేస్తామని హెచ్చరిస్తారు.

పైన ఇచ్చిన ఇ–మెయిల్‌ను ఈ రకమైన మోసానికి ఉదాహరణగా చెప్పుకోవచ్చు.

సైబర్ నేరస్థులు తరచూ ఇలాంటి పద్ధతులు ఉపయోగించి భద్రతా విషయాలలో రాజీ పడేటట్లు నమ్మిస్తారు.

➢ **ప్రజాదరణ పొందిన వెబ్‌సైట్‌లు లేదా కంపెనీల మాదిరి భ్రమకలిగించే విధంగా వుండే నకిలీలు**

ఇ–మెయిల్‌లో మోసం చేసే వారు గ్రాఫిక్ సహాయంతో తయారుచేసిన వెబ్ చిరునామాలు చట్టబద్ధత కలిగిన వెబ్‌సైట్‌లాగానే కనిపిస్తాయి.

అవి నిజమైన కంపెనీలవని నమ్మి క్లిక్ చేస్తే అవి నకిలీ వెబ్‌సైట్‌లకు మనల్ని తీసుకువెళ్ళతాయి.

సైబర్ నేరస్తులు కొద్దిపాటి మార్పులు చేసి పేరొందిన కంపెనీల పేరుతో వెబ్ చిరునామాలతో సైట్‌లను తయారుచేసి వాటిని వారి మోసాలకొరకు వినియోగిస్తారు.

అప్పుడప్పుడు సైబర్ నేరస్తులు ఫోన్ చేసి మీ కంప్యూటరుకు సంబంధించిన ఏమైనా సమస్యలు ఉంటే పరిష్కరిస్తామని అంటారు.

లేదా మీకు సాఫ్ట్‌వేర్ లైసెన్సులు అమ్ముతామని అంటారు.

గుర్తించుకోవలసిన అంశాలు

అంశం 1 : బ్రౌజర్‌లో వెబ్ చిరునామా (URL) ను ఒక దానికొకటి సరిచూసుకోవాలి.



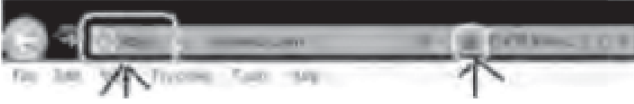
పై నెంబర్లతో మొదలయ్యే వెబ్‌సైట్‌లలో మీ సమాచారాన్ని ఎంటర్ చేయకండి.

అంశం 2 : స్పెల్లింగు తప్పులు ఏమైనా ఉన్నాయా అని యు.ఆర్.ఎల్ (URL) లో చూడండి

ఎల్లప్పుడూ యు.ఆర్.ఎల్ (URL) ను మీకై మీరు టైప్ చేయండి. కాపీ మరియు పేస్ట్ చేయకండి.



అంశం 3 : ఎల్లప్పుడూ ఆన్‌లైన్ బ్యాంకింగును భద్రత కలిగిన మార్గాలలోనే చేయాలి. అంటే చిరునామాకు ముందు ఉన్న పాడ్‌లాక్ మరియు భద్రతా ఛానల్‌లో సెక్యూర్డ్ బ్యాంకింగు ఉందా లేదా చూడాలి.



ఎల్లప్పుడూ https మరియు తాళం వేసివున్న గుర్తు ఉన్న వెబ్‌సైట్‌గా ఉందా లేదా గమనించి అలాంటి వాటిని మాత్రమే విశ్వసించాలి.

అంశం 4 : ఎల్లప్పుడూ ఇ–మెయిల్‌లో మీ ఆర్థికపరమైన, వ్యక్తిగత సమాచారం అడిగినప్పుడు ముఖ్యంగా అత్యవసరం అని అడిగినప్పుడు అలాంటి మెయిల్‌లను సందేహాస్పదంగా చూడాలి. ఎప్పుడైతే మెయిల్ పై సందేహం వచ్చిందో వెంటనే ఆ మెయిల్ ప్రశ్నావళికి సమాధానం ఇవ్వవద్దు. అటువంటి వెబ్‌సైట్‌లలో వివరాలు అందివ్వకూడదు. మీకు మెయిల్ పంపినవారిని వీలైతే సంప్రదించి మీకొచ్చిన సమాచారం మరియు వెబ్‌సైట్‌ల చట్టబద్ధతను నిర్ధారించుకోవలసి ఉంటుంది.

అంశం 5 : మీ వ్యక్తిగత క్రెడిట్ కార్డు / డెబిట్ కార్డు / బ్యాంకు సమాచారం అడిగిన ఇ–మెయిల్‌కు మీరు ఎప్పుడు స్పందించకండి.

చేయవలసినవి :

☑ ఎవరు పంపించారో తెలియకుండా మీ మెయిల్ బాక్సుకు, ఫేస్‌బుక్‌కు వచ్చిన అటాచ్‌మెంట్‌లను తెరవకండి. అలాగే ఫైళ్ళను డౌన్‌లోడు చేయకండి.

☑ మీరు మీ వ్యక్తిగత సమాచారం మరియు వివరాలు అందించే ముందు మిమ్మల్ని పంపమని కోరిన వారి ఈ మెయిల్ ఐ.డి ఏమిటో ఒకసారి పరిశీలనగా చూడండి.

☑ యాంటీ వైరస్, యాంటీ స్పైవేర్ మరియు ఫైర్‌వాల్ సాఫ్ట్‌వేర్‌లను వినియోగించండి. వాటిని ఎప్పటికప్పుడు తాజాగా వుంచుకోండి.

☑ మీ వెబ్ బ్రౌజరును ఎల్లప్పుడూ తాజాగా వుంచుకోవాలి మరియు ఫిషింగ్ ఫిల్టరును ఎనేబుల్ చేసుకొండి.

☑ మీకు ఒకవేళ ఏదైనా సందేహించే ఇ–మెయిల్ వచ్చినప్పుడు, దానికి సంబంధించిన కంపెనీకి ఫోన్ చేసి దానికి విశ్వసనీయత ఉందా? లేదా? అని ధృవీకరించుకోండి.

☑ వ్యక్తిగత, ఆన్‌లైన్ షాపింగ్ లాంటి వివిధ అవసరాలకు వేర్వేరు ఇ–మెయిల్ ఖాతాలను వినియోగించండి.

చేయకూడనివి :

☒ వ్యక్తిగత లేదా ఆర్థిక సమాచారం అడిగిన ఇ–మెయిల్ మరియు పాప్ – ఆప్ సమాచారాలకు మీరు సమాధానాలు ఇవ్వకండి.

☒ ఎవరికి మీ వ్యక్తిగత లేదా ఆర్థిక సమాచారాన్ని మరియు ఇతర విలువైన సమాచారాన్ని ఇ–మెయిల్ ద్వారా పంపకండి.

☒ మీరు ఊహజించనిది లేదా అవసరం లేని ఇ–మెయిల్ మరియు సామాజిక మాధ్యమ సందేశాలు వచ్చినప్పుడు మీరు దానిని క్లిక్ చేయకండి.

☒ మీకు చట్టబద్దం కాదని సందేహించిన ఇ–మెయిల్ ను తెరచి చూడకండి. ఒక వేళ అది విశ్వసనీయత ఉన్నదైతే నిజంగా అవసరమైనదైతే పంపిన వ్యక్తి మిమ్మల్ని వేరే విధంగా కలవడానికి ప్రయత్నిస్తారు.

☒ మీరు ఎదురుచూడని ఏదైనా ఇ–మేయిల్ అటాచ్‌మెంట్ తో వస్తే ముఖ్యంగా జిప్ ఫైళ్ళు, మరియు నెవర్ రన్. ఇఎక్స్ఇ (NEVERrun.exe) ఫైళ్ళను తెరవకండి.

☒ మీ వ్యక్తిగత విషయాలకు కంపెనీ ఇ–మెయిల్ చిరునామాను వాడకండి. స్పేమ్ (బల్క్) ఇ–మెయిల్ లను తెరవకండి.

☒ ఫిషింగుకు ప్రధాన వనరుగా ఉన్న సామాజిక వెబ్ సైట్ లలో మీకు సందేహం ఉన్న వీడియోలను లేదా ఫోటోలను తెరవకండి.

☒ ఫోన్‌లో మీ బ్యాంకు ఖాతా వివరాలు అడిగినప్పుడు దానికి మీరు వివరములు ఎప్పుడూ అందించకండి. ఇది విషింగ్‌కావచ్చు (వాయిస్ ఫిషింగ్)

☒ ఫిషింగ్ ఫోన్ కాల్ ల పట్ల జాగ్రత్తగా ఉండండి.

☒ మీరు వ్యక్తిగత సమాచారం అందించేందుకు వీలుగా మీకు ప్రైజ్ వచ్చిందని లేదా మీరు పోగొట్టుకున్న లేదా చోరీకి గురైనచో వాటి వివరాలు నిర్ధారించుకోవడానికి వివిధ రకాలుగా వివరాలు ఇవ్వమని సంక్షిప్త సమాచారం (SMS) లు ఏవైనా వస్తే వాటికి సమాధానం ఇవ్వకండి. ఎక్కువ భాగం ఫిషింగు పద్ధతి ఇలాగే ఉంటుంది.

ఇక్కడ కొన్ని ఫిషింగ్ పద్ధతులు ఇవ్వబడ్డాయి :

➲ సామాజిక నెట్‌వర్క్‌లే ఇప్పుడు ప్రధానంగా ఫిషింగు లక్ష్యంగా ఉన్నాయి. ఇందులోని వ్యక్తిగత సమాచారం దొంగిలించి ఫిషింగు పాల్పడేందుకు అనువుగా ఉండడం దీనికి ప్రధాన కారణం.

➲ ఇప్పుడూ బాగా ప్రాచుర్యంలో ఉన్న కొత్త ఫిషింగ్ పద్ధతి ఏమిటంటే టాబ్ నాబింగ్. ప్రస్తుతం ఎక్కువ టాబ్‌లు ఓపెన్ చేసుకొని వినియోగిస్తున్నారు. తనకు తెలియకుండానే గుట్టుచప్పుడు కాకుండా వినియోగదారుడుని ఫిషింగ్‌కు గురైన సైట్‌పై పనిచేసేటట్లు చేస్తుంది.

➲ వడబోతతో తప్పించుకోవడం (Filter Evasion)- ఫిషెర్స్ పదాలకు బదులు ఫోటో ఇమేజ్‌లను వాడుతున్నారు. దీనితో ఏంటి ఫిషింగు వడబోతలో సామాన్యంగా వచ్చే పదాలతో కూడిన ఫిషింగ్ ఇ–మెయిల్ లాగా అది దొరకడం లేదు.

➲ ఫోన్ ఫిషింగ్ (Phone Phishing) - అన్ని ఫిషింగ్ దాడులకు నకిలీ వెబ్‌సైట్ ఉండనక్కరలేదు. మీ ఖాతాలో ఏదైనా సమస్య ఉంటే ఫోన్ చేసి చెప్పమని బ్యాంకు నుండి సందేశం రావచ్చు.

ఒకవేళ నమ్మి వారు ఇచ్చిన ఫోన్ నెంబరుకు ఫోన్ చేస్తే (ఈ ఫోన్ ఫిషర్ మరియు వాయిస్ ఓవర్ సర్వీసు కలిగినదై ఉంటుంది). దీని ద్వారా అందించే సమాచారం ఖాతా వివరములు మరియు పిన్ వివరములు ఎంటర్ చేయమని అడుగుతారు. ఫిషర్ కొన్నిసార్లు నకిలీ గుర్తింపు సంఖ్యను వాడి అది నమ్మకమైన సంస్థ నుండే వచ్చిందని బుకాయిస్తారు.

➲ బ్యాంకు వెబ్‌సైట్ లాగానే వెబ్‌సైట్ ఓపెన్ చేయగానే కన్పించి ఒక పాప్అప్ సందేశం మన ఖాతాకు చెందిన వ్యక్తిగత వివరములు ఎంటర్ చేయమని కోరవచ్చు. ఇది విశ్వసనీయత కలిగిన వెబ్‌సైట్‌లాగానే కనిపిస్తుంది.

ఏదైనా సమాచారం వచ్చినప్పుడు అది ఫిషింగ్‌దేనని ఎలా గుర్తించడం.

➲ సాధారణంగా ఫిషింగ్ ఇ-మెయిల్‌లు గ్రామరు తప్పులతోనూ మరియు చిందరవందర అక్షరాలతోను (overlapped text) నిండి ఉంటుంది.

➲ ఒకవేళ పరీక్షించదలచుకుంటే ముందుగా సరైన సమాచారం కాకుండా తప్పుడు సమాచారాన్ని ఎంటర్ చేయండి.

నేను అనుకోకుండా ఫిషింగ్ మోసానికి సమాచారం ఇచ్చానని తెలిస్తే ఏం చేయాలి?

➲ మీరు ఒకవేళ ఫిషింగ్ మోసానికి అనుకోకుండా మీ వ్యక్తిగత మరియు ఆర్థిక సమాచారం ఇచ్చి ఉంటే ఆర్థిక నష్టాలు జరుగకుండా ఈ క్రింది జాగ్రత్తలు తీసుకోండి.

➲ మీ ఆన్‌లైన్‌కు చెందిన అన్నిరకాల పాస్‌వర్డ్‌లను మరియు పిన్‌లను వెంటనే మార్చివేయండి.

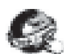
➲ మీ క్రెడిట్ రిపోర్టుకు మోసం జరిగినట్లు హెచ్చరిక సందేశాన్ని పెట్టండి. మీకు ఏమి చేయాలో తెలియకపోతే బ్యాంకును కలిసి మరియు మీ ఆర్థిక సలహాదారుడిని సంప్రదించి ఏమి చేయాలో సలహా తీసుకోండి.

➲ మీ బ్యాంకు లేదా ఆన్‌లైన్ వ్యాపారులను నేరుగా సంప్రదించండి. అంతేగాని మీకు వచ్చిన మోసపూరిత వెబ్‌లింకులను, ఇ-మెయిల్‌లను అనుసరించకండి.

➲ మీరు ఖర్చు పెట్టని లేదా మళ్ళీ మళ్ళీ నమోదు అయిన అంశాలు ఏవైనా ఉన్నాయేమోనని తరచుగా మీ బ్యాంకు మరియు క్రెడిట్ కార్డు లావాదేవీల వివరములు సమీక్షించుకోండి.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

14. సిమ్ స్వాప్

ఎన్నో ఏళ్ళుగా వాడుతున్న సిమ్‌కార్డు మీ ఫోన్‌లోనే ఉంటుంది... మాట్లాడు తుంటారు... ఆన్‌లైన్ బ్యాంకింగ్ చేస్తుంటారు.

వాలెట్లు వాడేస్తుంటారు... ఉన్నట్లుండి సిమ్ వేరొకరి చేతికి వెళ్తుంది... అనుకోకుండా నెట్‌వర్క్ డిసేబుల్ అవుతుంది.

అదెలా సాధ్యం అంటారా? అదే "సిమ్ స్వాప్". ఓ పథకం ప్రకారం హ్యాకర్లు వేసే స్కెచ్! ఇప్పుడిదే హ్యాకర్లు విసిరే మోసపూరిత పాచిక!!

ఏమిటీ సిమ్ స్వాప్ :

నూతన పద్ధతి ద్వారా సెల్‌ఫోన్ వినియోగదారులను సులువుగా మోసం చేస్తున్నారు. దీనివల్ల బ్యాంకులోని తమ ఖాతాల నుంచి డబ్బు పోగొట్టు కుంటున్నారు.

ఈ మోసాలబారిన కేవలం నిరక్షరాస్యులే కాకుండా... టెకీలు కూడా పడుతున్నారంటే ఏ స్థాయిలో వీటిపై అవగాహన ఉందో తెలసుకోవచ్చు.

అన్నింటికీ కీలకం :

ఈ మధ్య కాలంలో బ్యాంకు ఖాతాల లావాదేవీల వివరాలు, సంక్షిప్త సందేశాలు మొబైల్ నంబర్లకే వస్తున్నాయి. అధీకృత నంబరుకే ఓ.టి.పి. వివరాలు వస్తాయి.

ఇంతటి ముఖ్యమైన దానికి సంబంధించి పెద్దగా అవగాహన లేకపోవడంతో అందరు తేలికగా మోసపోతున్నారు.

మీకు వచ్చిన కాల్స్ అధికారికమైనవే అనుకున్నారు. వివరాలు పంచుకున్నారు. కానీ కొన్ని రోజులకే వారు వాడుతున్న ఫోన్ నెంబర్ హ్యాకర్ చేతికి వెళ్ళింది.

వారి ఫోన్‌లలో నెట్‌వర్క్ డిసేబుల్ అయిపోయింది.

నింపాదిగా నెట్‌వర్క్ ప్రొవైడర్‌ని కలిసిలోపే బ్యాంక్ అకౌంట్‌లోని సొమ్మంతా ఖాళీ... అంతేనా క్రెడిట్ కార్డులు నిల్ అయిపోయాయి. వాలెట్స్‌లో ఈ డబ్బంతా మాయం.

చేసేది లేక సైబర్ క్రైమ్‌ని ఆశ్రయిస్తే అప్పుడు తెలిసింది. వారి సిమ్ వేరొకరి సొంతం అయిందని. దీనినే "సిమ్‌స్వాప్" అంటారని.

పక్కా ప్రణాళిక :

సిమ్‌స్వాప్ చేసేందుకు హ్యాకర్లు ఒక పక్కా ప్రణాళిక అమలు చేస్తారు. వ్యక్తుల్ని లక్ష్యంగా చేసుకున్నాక సోషల్‌లైఫ్‌లో నిఘా పెడతారు.

దీనిని అంతా "సోషల్ ఇంజనీరింగ్" అంటున్నారు.

మీ ప్రొఫైల్‌ని జల్లెడ పడతారు. వ్యక్తిగత వివరాలు ఎక్కడ కనిపించినా నోట్ చేసుకుంటారు.

ఒక వేళ మీ ప్రైవసీ సెట్టింగ్స్ పక్కాగా ఉంటే మీ నెట్‌వర్క్‌లోని స్నేహితుల ప్రొఫైల్స్‌ని ఎంపిక చేసుకుంటారు. ఎవరికైతే ప్రైవసీ సెట్టింగ్స్ సరిగా లేవో... వారి సోషల్ వాల్స్‌పై మీకు సంబంధించిన డేటాని కనిపెట్టడం పెద్ద కష్టమేమి కాదు.

మెయిల్ ఐ.డి., పేర్లు, ఫ్యామిలీ వివరాలు, అడ్రస్సులాంటి డేటాని క్షుణ్ణంగా సేకరిస్తారు. ఆ మొత్తం డేటాతో మీరు వాడే పాస్‌వర్డ్‌లు ఏమైనా ఉంటాయో కూడా ఊహించగలరు. అంత కట్టుదిట్టమైన సమాచారం సేకరించాకే ఫోన్ వస్తుంది.

మీరు వాడుతున్న నెట్‌వర్క్ కస్టమర్ నుంచే మాట్లాడుతున్నాం అని మాట కలుపుతారు. లేని నెట్‌వర్క్ సమస్యని ఉన్నట్లు నమ్మిస్తారు.

లేదంటే మీకు ఇష్టమైన కాలర్‌ట్యూన్ యాక్టివేట్ చేసుకోమని మెసేజ్ పంపుతారు. అందుకు ప్రత్యేక కోడ్‌ని కస్టమర్‌కేర్‌కి పంపమని కోరుతారు.

- ఆధార్ సెంటర్ నుండి మాట్లాడుతున్నాం, మీ ఆధార్ నెంబరుతో సమస్య వస్తోంది. దీనికి ఆధార్‌కి అనుసంధానం చేసిన ఫోన్ నెంబర్‌కి కూడా ఓటిపి రావడంలోను భవిష్యత్తులో సమస్యలు రావచ్చు. అందుకే సర్వీసుని అప్‌డేట్ చేస్తున్నాం. మేము మీకు పంపే ప్రత్యేక నెంబర్‌ని మీ కస్టమర్ కేర్ నంబరుకు పంపితే చాలు.
- కస్టమర్ కేర్ నుంచి మాట్లాడుతున్నాం. మీ ఫోన్ నెట్‌వర్క్‌లో ఏమైనా సమస్యలున్నాయా? అప్పుడప్పుడు సిగ్నల్ జామ్ అవుతోందా? కాల్‌డ్రాప్స్ అవుతున్నాయా? మెసేజ్‌లు రావడం లేదా? అయితే మీ సిమ్ వెనుకనున్న 20 అంకెల సంఖ్యను చెప్పండి.

  మేము సరిచేసి నెట్‌వర్క్‌ని రిపోర్ట్ చేస్తాం. ఈ క్రమంలో కొన్ని గంటలపాటు మీ సిమ్ డిసేబుల్ అయినా చింతించకండి. తిరిగి రీ స్టోర్ అవుతుంది. అని మోసగాళ్ళు ఫోన్‌చేసి కోరగా అది నమ్మి ఒక వ్యక్తి తన సిమ్‌కార్డు వెనుకనున్న నెంబర్ చెప్పాడు.

వాట్సప్ మెసేజ్ :

మీకు ఇష్టమైన పాటను కాలర్‌ట్యూన్‌గా పెట్టుకోవాలా? అయితే ఈ నెంబర్ కోడ్‌ని కస్టమర్ కేర్‌కి ఫార్వర్డ్ చేయండి. వెంటనే మీకు ఇష్టమైన కాలర్ ట్యూన్ ఉచితంగా యాక్టివేట్ అవుతుంది.

మొదటి పది మందికే ఈ ఆఫర్ అని వెంటనే శిరీష తనకు ఇష్టమైన పాటకోసం కోడ్‌ని కస్టమర్‌కేర్‌కు పంపింది.

మీ అంతట మీరే కోడ్‌ని పంపేలా నమ్మిస్తారు. అంతే... కంట్రోల్ వారి చేతిలోనికి వచ్చేస్తుంది. మీ సిమ్ వారిదైపోతుంది.

ఒకవైపు మిమ్మల్ని నియంత్రిస్తూనే నెట్‌వర్క్ ప్రొవైడర్‌తో మాట్లాడుతూ ఖాళీ సిమ్‌లోకి

మీ నెంబర్ యాక్టివేట్ అయ్యేలా స్కెచ్ వేస్తారు. కొద్ది గంటలలోనే నెంబరు పూర్తిస్థాయిలో వారిది అయిపోతుంది. అంతే... సోషల్ ఇంజనీరింగ్ ద్వారా సేకరించిన డేటా ఆధారంగా కొల్లగొట్టడం మొదలు పెడతారు. ఓ.టి.పి.లు, పిన్ నెంబర్లు అన్నీ ఫోన్ నుంచేగా వచ్చేది. క్షణాల్లో అన్నింటిపై యాక్సెస్ సాధించి తేరుకునేలోపే తుడిచిపెట్టేస్తారు.

"సిమ్ స్వాప్ పద్ధతి"లో చేసే మోసాలకు ఎక్కువగా వయస్సు మళ్ళిన వారినే లక్ష్యంగా చేసుకుంటున్నారు. ఆ నెంబర్ ద్వారా నెట్‌వర్క్ ప్రొవైడర్‌ని ఫోన్‌చేసి మా సిమ్ పాడయ్యిందని, లేదంటే పోయిందని చెబుతారు. పాత నెంబర్‌నే క్రొత్త సిమ్‌లోకి జతచేసి ఇవ్వాలని కోరుతారు. అధికారిక యూజర్లకు అనుమానం రాకుండా పలు నెంబర్లనుంచి పదే పదే కాల్స్ చేస్తారు. విసుగొచ్చేలా చేసి చేసిన మోసాన్ని గుర్తించకుండా జాగ్రత్త పడతారు. ఆ విసుగులో కస్టమర్ కేర్ నుంచి వచ్చే నోటిఫికేషన్ అలర్ట్‌లను పెద్దగా పట్టించుకోరు.

మరో పద్ధతిలో.... సిమ్ పోయిందని పోలీస్ స్టేషన్‌కు వెళ్ళి ఫిర్యాదు చేస్తారు. అక్కడ ఇచ్చిన ఫిర్యాదు కాపీ ఆధారంగా నెట్‌వర్క్ ఆపరేటర్ వద్దకు వెళ్ళి క్రొత్తసిమ్ కోసం ధరఖాస్తు చేస్తారు. దీనికోసం ఇచ్చే ఆధార్, నివాస ధృవీకరణ పత్రాలు నకిలీవి సమర్పిస్తారు. ఫోటోను మార్చి ఇస్తారు. వీటిని పరిశీలించి సిమ్ ఇస్తారు.

మన వద్దఉన్న అసలు సిమ్‌ను బ్లాక్‌చేసి మోసగాడికి మంజూరు చేసిన సిమ్‌ను యాక్టివేట్ చేస్తారు. దీనితో అప్పటినుండి సిమ్‌కు వచ్చే ఓ.టి.పి., బ్యాంకుకు సంబంధించిన సందేశాలు క్రొత్తదానికి వెళ్తాయి. దీని ఆధారముతో డబ్బు కొట్టేస్తారు.

నరేంద్రకి ఓ ఫోన్‌కాల్ :

'ఆధార్ సెంటర్ నుంచి మాట్లాడుతున్నాం. మీ ఆధార్ నంబర్‌తో సమస్య వస్తోంది. దీంతో ఆధార్ కి అనుసంధానం చేసిన ఫోన్ నెంబర్‌కి కూడా ఓటీపీ రావడంలోనూ భవిష్యత్తులో సమస్యలు రావచ్చు. అందుకే సర్వీసుని అప్‌డేట్ చేస్తున్నాం. మేము మీకు పంపే ప్రత్యేకనెంబర్‌ని మీ కస్టమర్ కేర్ నంబరుకు పంపితే చాలు.

నారాయణకి ఫోన్ వచ్చింది :

'కస్టమర్ కేర్ నుంచి మాట్లాడుతున్నాం. మీ ఫోన్ నెట్‌వర్క్‌లో ఏమైనా సమస్యలున్నాయా? అప్పుడప్పుడూ సిగ్నల్స్ జామ్ అవుతోందా? కాల్స్ డ్రాప్ అవుతున్నాయా? మెసేజ్‌లు రావడం లేదా? అయితే, మీ సిమ్ వెనుకున్న 20 అంకెల సంఖ్యను చెప్పండి. మేం సరిచేసి నెట్‌వర్క్‌ని రీస్టోర్ చేస్తాం. ఈ క్రమంలో కొన్ని గంటలపాటు సిమ్ డిసేబుల్ అయినా చింతించకండి. తిరిగి రీస్టోర్ అవుతుంది' అని నారాయణ వెనకున్న నెంబర్ చెప్పారు.

శిరీషకి వాట్సాప్ మెసేజ్ :

'మీకు ఇష్టమైన పాటని కాలర్ ట్యూన్‌గా పెట్టుకోవాలా? అయితే ఈ నెంబర్ కోడ్‌ని కస్టమర్ కేర్‌కి ఫార్వర్డ్ చేయండి. వెంటనే మీకు ఇష్టమైన కాలర్ ట్యూన్ ఉచితంగా యాక్టివేట్ అవుతుంది. మొదటి పదిమందికే ఈ ఆఫర్ అని' వెంటనే శిరీష తనకు ఇష్టమైన

పాట కోసం కోడ్‌ని కస్టమర్ కేర్‌కి పంపింది. నారాయణ, నరేంద్ర, శిరీష... వీరికొచ్చిన కాల్స్ అధికారికమైనవే అనుకున్నారు. వివరాలు పంచుకున్నారు. కానీ కొన్ని రోజులకే వారు వాడుతున్న ఫోన్ నెంబర్ హ్యాకర్ చేతికి వెళ్ళింది.

వారి ఫోన్‌లలో నెట్‌వర్క్ డిసేబుల్ అయిపోయింది. నింపాదిగా నెట్‌వర్క్ ప్రొవైడర్‌ని కలిసే లోపే బ్యాంకు ఎకౌంట్‌లోని సొమ్మంతా ఖాళీ... అంతేనా... క్రెడిట్ కార్డులు నిల్ అయిపోయాయ్... వాలెట్స్‌లో ఈ–డబ్బంతా మాయం.

చేసేది లేక సైబర్ క్రైమ్‌ని ఆశ్రయిస్తే అప్పుడు తెలిసింది. వారి సిమ్ వేరొకరి సొంతం అయిందని, దీన్నే "సిమ్ స్వాప్" అంటారని. మరి మీ సంగతేంటి? ఇలాంటి కాల్స్ మీకెప్పుడైనా వచ్చాయా?

పక్కా ప్రణాళిక :

సిమ్ స్వాప్ చేసేందుకు హ్యాకర్లు ఓ పక్కా ప్రణాళిక అమలుచేస్తారు. వ్యక్తుల్ని లక్ష్యంగా చేసుకున్నాక సోషల్ లైఫ్‌లో నిఘా పెడతారు. దీన్నే "సోషల్ ఇంజనీరింగ్" అంటున్నారు. ప్రొఫైల్స్‌ని జల్లెడపడతారు. వ్యక్తిగత వివరాలు ఎక్కడ కనిపించినా నోట్ చేసుకుంటారు.

ఒకవేళ మీ ప్రైవసీ సెట్టింగ్స్ పక్కాగా ఉంటే మీ నెట్‌వర్క్‌లోని స్నేహితుల ప్రొఫైల్స్‌ని ఎంపిక చేసుకొంటారు. ఎవరికైతే ప్రైవసీ సెట్టింగ్స్ సరిగా లేవో... వారి సోషల్ వాల్స్ పై మీకు సంబంధించిన డేటాని కనిపెట్టడం పెద్ద కష్టమేం కాదు. మెయిల్ ఐడీ, పేర్లు, ఫ్యామిలీ వివరాలు, అడ్రస్... లాంటి డేటాని క్షుణ్ణంగా సేకరిస్తారు.

ఆ మొత్తం డేటాతో మీరు వాడే పాస్‌వర్డ్‌లు ఏమై ఉంటాయో కూడా ఊహించగలరు. అంత కట్టుదిట్టమైన సమాచారం సేకరించాకే ఫోన్ వస్తుంది. మీరు వాడుతున్న నెట్‌వర్క్ కస్టమర్ కేర్ నుంచే మాట్లాడుతున్నాం అని మాట కలుపుతారు. లేని నెట్‌వర్క్ సమస్యని ఉన్నట్టుగా నమ్మిస్తారు.

లేదంటే మీకు ఇష్టమైన కాలర్ ట్యూన్ యాక్టివేట్ చేసుకోమని మెసేజ్ పంపుతారు. అందుకు ప్రత్యేక కోడ్‌ని కస్టమర్ కేర్‌కి పంపమని కోరతారు. మీ అంతట మీరే కోడ్‌ని పంపేలా నమ్మిస్తారు. అంతే... కంట్రోల్ వారి చేతిలోకి వచ్చేస్తుంది. మీ సిమ్ వారిదైపోతుంది. ఒకవైపు మిమ్మల్ని నియంత్రిస్తూనే నెట్‌వర్క్ ప్రొవైడర్‌తో మాట్లాడుతూ ఖాళీ సిమ్... మీ నెంబర్ యాక్టివేట్ అయ్యేలా .... .. కొద్ది గంటల్లోనే నెంబర్...

'సిమ్ స్వాప్ పద్ధతిలో చేసే మోసాలకు ఎక్కువగా వయస్సు మళ్ళిన వారినే లక్ష్యంగా చేసుకుంటున్నారు. 'ఫోన్ కాల్స్ ఎక్కువగా డ్రాప్ అవుతున్నాయా? మెసేజ్‌లు రావడం లేదా? నెట్‌వర్క్ సరిగా ఉండడం లేదా?' అని మాట్లాడుతూ సిమ్ వెనకున్న 20 అంకెల నెంబర్‌ని సేకరించే ప్రయత్నం చేస్తారు. ఆ నెంబర్ ద్వారా నెట్‌వర్క్ ప్రొవైడర్‌ని ఫోన్ చేసి మా సిమ్ పాడయ్యిందని... లేదంటే పోయిందని చెబుతారు. పాత నెంబర్‌నే కొత్త సిమ్‌లోకి జత చేసి ఇవ్వాలని కోరతారు.

అధికారిక యూజర్లకు అనుమానం రాకుండా పలు నెంబర్ల నుంచి పదేపదే కాల్స్ చేస్తారు. విసుగొచ్చేలా చేసి చేస్తున్న మోసాన్ని గుర్తించకుండా జాగ్రత్త పడతారు. ఆ విసుగులో కస్టమర్ కేర్ నుంచి వచ్చే నోటిఫికేషన్ అలర్ట్‌లను పెద్దగా పట్టించుకోరు.

జాగ్రత్తలు :

- ఏ కారణం లేకుండా మీ మొబైల్ నెంబర్ పనిచేయకుండా డిసేబుల్ అయితే మళ్లీ వస్తుందిలే అని వేసి చూడొద్దు. వెంటనే మీ నెట్‌వర్క్ టెలికాం ఆపరేటర్‌ని సంప్రదించాలి. నెంబర్‌ని మీ కోరిక మేరకు బ్లాక్‌లోనే ఉంచమని కోరాలి.
- ఆన్‌లైన్ బ్యాంకింగ్‌కి విడిగా మెయిల్ ఐడీని క్రియేట్ చేసుకుంటే మంచిది. దాన్ని మరే ఇతర సోషల్ మీడియా నెట్‌వర్క్‌లలో వాడొద్దు.
- నిర్ణీత తేదీల్లో బ్యాంకు స్టేట్‌మెంట్స్‌ని జనరేట్ చేసుకుని నిశితంగా పరిశీలించండి. మీ ప్రమేయం లేకుండా ఏవైనా లావాదేవీలు జరిగితే గుర్తించడం సులభం అవుతుంది.
- గుర్తు తెలియని నంబర్ల నుంచి వచ్చే కాలర్లకు మీ వ్యక్తిగత వివరాల్ని ఎట్టి పరిస్థితుల్లోనూ షేర్ చేయొద్దు. ఏ బ్యాంకింగ్ సంస్థగానీ, మరే ఇతర ఆన్‌లైన్ సర్వీసులుగానీ వ్యక్తిగత వివరాల్ని ఫోన్ కాల్స్ ద్వారా కోరరు అనే విషయాన్ని గుర్తుంచుకోవాలి.
- కస్టమర్ కేర్ నుంచి మాట్లాడుతున్నాం అని చెబుతూ మీ సిమ్ వెనకున్న 20 అంకెల నెంబర్‌ని తెలపమని కోరినట్లయితే అనుమానించాల్సిందే.
- ఆన్‌లైన్ సర్వీసులకు వాడే 'సెక్యూరిటీ క్వశ్చన్స్'ని ఇతరులతో పంచుకోవద్దు. అనివార్యమైన పబ్లిక్ ప్రాంతాలలో వాటి గురించి చర్చించే ప్రయత్నం చేయొద్దు.
- గుర్తు తెలియని వ్యక్తులు, సంస్థల నుంచి వచ్చే మెయిల్స్‌కి స్పందించొద్దు. లింక్‌లను తాకొద్దు.
- బ్యాంకింగ్ వెబ్‌సైట్‌ని అడ్రస్ బార్‌లో స్పష్టంగా టైప్‌చేసి మాత్రమే లాగిన్ అవ్వాలి. బుక్ మార్క్ చేశాం కదా అనుకోవద్దు. ఎందుకంటే... కొన్ని రకాల మాల్వేర్లు సిస్టంలో చేరి పెట్టుకున్న బుక్‌మార్క్‌లను ఫిషింగ్‌సైట్‌లుగా మార్చేస్తాయి.
- ఫోన్లలో థర్డ్ పార్టీ యాప్‌లను ఇన్‌స్టాల్ చేసేటప్పుడు ఒకటి రెండు సార్లు చెక్ చేసుకోండి.
- వాట్సాప్‌కి వచ్చే ఆఫర్ మెసేజ్‌లను పట్టించుకోవద్దు. వాటిల్లో లింక్‌లను క్లిక్ చేస్తే హ్యాకర్ గాలానికి చిక్కినట్టే.
- పుట్టిన రోజు, పెళ్ళి రోజు, మరేదైనా శుభకార్యాలకు సంబంధించిన తేదీలు, ఇష్టమైన రంగులు, ముద్దు పేర్లు, పెంపుడు జంతువుల పేర్లు .... లాంటి వ్యక్తిగత వివరాల్ని సోషల్ నెట్‌వర్క్ ప్రొఫైళ్ళలోగానీ, వాల్స్‌పైన గానీ పంచుకోవద్దు.
- ఆర్థిక లావాదేవీలకు సంబంధించిన ఆన్‌లైన్ వ్యవహారం ఏదైనా ఫోన్‌కి టెక్ట్స్ మెసేజ్‌తో పాటు ఈ-మెయిల్‌కి సందేశం వచ్చేలా అలర్ట్‌ని సెట్ చేసుకోవాలి.
- అన్ని బ్యాంకింగ్ సర్వీసులకు ఒకే మొబైల్ నెంబరును వాడొద్దు. వేరు వేరు రకాల నంబర్లను వాడండి. దీంతో అంతగా నష్టపోకుండా చూసుకోవచ్చు.

- బ్యాంకులు కొత్త పద్ధతులలో అందుబాటులోకి తెస్తున్న 'స్మార్ట్' పిన్‌లు, స్మార్ట్ పాస్‌వర్డ్‌లను వాడడం అలవాటు చేసుకోవాలి.
- ఎప్పటికప్పుడు బ్యాంకింగ్ వెబ్‌సైట్‌ల పాస్‌వర్డ్‌లు మార్చేస్తుండాలి.
- వాడుతున్న యాంటీవైరస్‌లను ఎప్పటికప్పుడు అప్‌డేట్ చేస్తుండాలి.
- ఇతరులు వాడే కంప్యూటర్లు, నెట్‌వర్క్‌కి అనుసంధానమై ఉన్నవాటిలో వ్యక్తిగతమైన వివరాలు, పాస్‌వర్డ్‌లను సేవ్ చేయొద్దు.

ఆధార్‌తోనే ఎక్కువ మోసాలు :

'సిమ్ స్వాప్' ద్వారా చేసే మోసాలు ఎక్కువగా ఆధార్ నంబర్‌ని అప్‌డేట్ చేయాలనే కోణంలోనే చోటు చేసుకుంటాయి. దేశవ్యాప్తంగా ఇలాంటి కేసులే ఎక్కువ. హ్యాకర్ పంపే నంబర్ ఏంటంటే... తను తీసుకున్న ఖాళీ సిమ్ వెనక ఉండే 20 అంకెల నంబర్, యూజర్ ఎప్పుడైతే వాడుతున్న నెంబర్ నుంచి కస్టమర్ కేర్‌కి ప్రత్యేక నెంబర్‌ని ఫార్వర్డ్ చేస్తాడో హ్యాకర్ దగ్గరున్న ఖాళీ సిమ్‌లోకి యూజర్ వాడుతున్న ఫోన్ నెంబర్ నిర్ణీత సమయానికి యాక్టివేట్ అవుతుంది.

ఆ తర్వాత యూజర్ ఫోన్ లోని సిమ్ డీయాక్టివేట్ అవుతుంది. ఇవే కాదు, మరెన్నో రకాలుగా వల పన్నేందుకు సైబర్ మోసగాళ్ళు సిద్ధంగా ఉంటారు. ఎలా ఉంటాయంటే... ఇన్‌కంట్యాక్స్ ఓ ఇరవై వేలు వచ్చాయని, త్వరలోనే మీ బ్యాంకు ఖాతాకి జమ అవుతాయని చెబుతారు. అకౌంట్ నంబర్‌ని ఒకసారి చెక్ చేసుకోమని చెబుతారు. అందుకు పంపిన మెసేజ్‌లో ప్రత్యేక లింక్‌ని జతచేస్తారు. యూజర్లు అది నమ్మి లింక్ పై క్లిక్‌చేసి లాగిన్ అయితే... ఇరవై వేలు డిపాజిట్ అవ్వడం కాదు. అకౌంట్‌లో డబ్బులు హాంఫట్ అవుతుంది.

ఈ సిమ్ స్వాప్ మోసాల్ని అరికట్టేందుకు ట్రాయ్ కూడా 24 గంటలుపాటు ఎలాంటి ఎస్.ఎం.ఎస్‌లు వెళ్ళకుండా (ఇన్‌కమింగ్, అవుట్‌గోయింగ్) బ్లాక్ చేసేలా చర్యలు తీసుకుంది. దీనితో యూజర్లు అప్రమత్తమయ్యేందుకు వీలుంటుంది.

ఏవైనా నంబర్లు ఫార్వర్డు చేయాలని కోరుతూ మెసేజ్‌లు వస్తే స్పందించవద్దు. ప్రత్యేక ఆఫర్లంటూవచ్చే మెసేజ్‌ల్లోని గుర్తు తెలియని నెంబర్లకు ఫోన్ చేయొద్దు. డయల్ చేసిన నెంబర్ రీడైరక్ట్ అయ్యి హ్యాకర్ గూటికి కాల్ వెళ్తుంది.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

15. విదేశీ బ్యాంకుల్లో నిధులు ఉన్నాయని దీనికి వారసులు మీరే అని ఎర

మీకు విదేశాలల్లో బంధులువులు ఉన్నారా? వారు అర్ధాంతరంగా చనిపోయి మీ పేరుమీద లక్షల పౌండ్లు ఆస్తి రాసిచ్చారు. వారి బ్యాంకు ఖాతాల్లో పౌండ్లను మీకు ఇస్తామంటూ మోసగాళ్ళు మెయిల్స్ లేదా ఫోన్లు చేస్తున్నారు. వీటిలో రెండు ప్రశ్నలైనా సరే మీకు ఎదుర్కొని ఉంటే మీరు సైబర్ నేరస్థుల ఉచ్చులో పడినట్లే. అయాచితంగా డబ్బు వస్తుందంటే ముందూ వెనుకా అలోచించకుండా స్పందించే బలహీనతను సొమ్ము చేసుకొనేందుకు సైబర్ నేరస్తులు లక్షల పౌండ్లు పంపుతామంటూ మెయిల్స్ చేస్తున్నారు.

లండన్ బ్యాంకులో భారత సంతతికి చెందిన వైద్యనిపుణుడి ఖాతాలో 3 లక్షల పౌండ్లు (2.1 కోట్లు) ఉన్నాయని, ఆయన వారసురాలిగా నటిస్తే చెరో 1.5 లక్షల పౌండ్లు పంచుకుందామని నగరానికి చెందిన ఒక యువతిని ఒక నైజీరియన్ మోసం చేశాడు.

డాక్టర్ ఫెడరిక్ పేరుతో పరిచయం చేసుకున్న అతను ఆమె వద్ద నుంచి విడతల వారీగా లక్షల మొత్తంలో స్వాహా చేశాడు. తాను స్పెయిన్ బ్యూరీ బ్యాంక్ మేనేజర్నని, కొద్ది రోజుల క్రితం డాక్టర్ చనిపోయాడని, ఆయన ఖాతాలో 3 లక్షల పౌండ్లు గుర్తించానని మెయిల్లో పేర్కొన్నారు.

మీరు చనిపోయిన వ్యక్తికి వారుసురాలినంటూ బ్యాంకుకు పత్రాలు పంపితే చాలని మెయిల్ ద్వారా వివరించారు. నకిలీ వారసత్వ ధ్రువీకరణ పత్రాలు పంపించి బ్యూరీ బ్యాంకుకు మెయిల్ చేయాల్సిందిగా సూచించాడు. మెయిల్ పంపిన రెండు రోజులకే ఆ మహిళ ఖాతాలో రూ. 3 లక్షల పౌండ్లు జమ అయినట్లు సందేశం వచ్చింది.

తన ఖాతాలో అవి లేకపోవడంతో ఆ మోసగానికి ఫోన్చేయగా.... స్టాండర్డ్ ఛార్టెడ్ బ్యాంక్ పేరుతో తాత్కాలిక ఖాతాను బ్యూరీ బ్యాంక్ అధికారులే తెరిచారని ఇందుకు సంబంధించిన లింక్ను పంపించారని వివరించాడు. ఆ తరువాత ఆ మహిళ తన మెయిల్ చూసుకోగా... అందులో స్టాండర్డ్ ఛార్టెడ్ బ్యాంకు తాత్కాలిక ఖాతా వివరాలు ఉన్నాయి. వాటిని తెరిచేందుకు ప్రయత్నించగా రూ. 74 వేలు జమ చేయాలని పేర్కొంది.

రూ. 74 వేలు జమచేసి మళ్ళీ ఖాతాను తెరిచేందుకు ప్రయత్నించగా ప్రోసెసింగ్ రుసుం రూ. 1.75 లక్షలు చెల్లించాలని సందేశం వచ్చింది. ఆ మొత్తము జమ చేశాక ఆర్థిక విభాగం ఖర్చులంటూ మరోసారి సందేశం రాగా రూ.64 వేలు చెల్లించింది.

అనంతరం ఖాతా వివరాలు తెలుసుకునేందుకు ప్రయత్నించగా శాశ్వత ఖాతాకు మార్చుతున్నామని ఇందుకోసం రూ. 1 లక్ష జమచేయాలని మెయిల్ వచ్చింది. చివరకు మోసపోయానని గ్రహించిన యువతి సైబర్ క్రైమ్ పోలీసులకు ఫిర్యాదు చేసింది.

16. మీతోనే తప్పు చేయిస్తారు...

మీ అకౌంట్‌లోని డబ్బును దోచేస్తారు

ఆ ప్రాంతమంతా అంతే...

జార్ఖండ్‌లోని పశ్చిమ బెంగాల్ వెళ్ళే మార్గంలో ఉన్న ప్రాంతం జామ్‌తార.

ల్యాప్‌టాప్స్, సెల్‌ఫోన్స్‌లతో కూర్చునే ఈ ప్రాంత యువత ఇప్పుడు దేశ వ్యాప్తంగా అనేక మందికి గాలం వేస్తున్నారు.

జిల్లాలో నమోదవుతున్న ఈ కార్డ్ క్రైమ్‌లలో 98% ఈ ప్రాంతానికి చెందిన వారే నిందితులు.

బ్యాంకుల్లో క్రిందిస్థాయి ఔట్ సోర్సింగ్ ఉద్యోగులతో పాటు అనేక మార్గాల ద్వారా డెబిట్ / క్రెడిట్ కార్డుల డేటా సేకరిస్తున్న వీరు వాటి ఆధారంగా అసలు అంకానికి తెరలేపుతున్నారు. బోగస్ పేర్లు, చిరునామాలతో తీసుకునే జమ్‌తార యువకులు వీటిని వినియోగించి కార్డుల డేటాలోని ఫోన్‌నెంబరుకు కాల్‌చేస్తుంటారు.

ఒకప్పుడు హిందీ, ఇంగ్లీషు భాషల్లో సంభాషిస్తూ తాము బ్యాంక్ మేనేజర్లమని పరిచయం చేసుకుని కార్డు వివరాలతో పాటు ఓ.టి.పి.లు సంగ్రహించేవారు.

అయితే టార్గెట్ చేసిన వారిలో కొందరికి భాష అర్థం కావట్లేదనే ఉద్దేశంతో స్థానిక భాషలపై దృష్టి పెట్టినట్లు పోలీసులు అనుమానిస్తున్నారు.

వివిధ మార్గాలలో నేర్చుకుంటూ...

వీరు తెలుగుతోపాటు వివిధ స్థానిక భాషలను కూడా అనేక మార్గాలలో నేర్చుకుంటున్నట్లు పోలీసులు అనుమానిస్తున్నారు.

ఇంటర్‌నెట్‌తో పాటు కొన్ని పుస్తకాల ద్వారా నేర్చుకుంటున్నారని, వారు వినియోగిస్తున్న పదాలు, ఉచ్ఛారణ శైలిని పరిశీలిస్తే ఈ విషయం అర్థము అవుతుందని అంటున్నారు.

మధ్యతరగతికి చెందిన వారు వీరి నుంచి ఫోన్‌లు అందుకున్నప్పుడు స్థానిక భాషలో మాట్లాడడంతో నిజమే అని నమ్ముతున్నారు.

అప్‌డేట్, లింకేజీ పేర్లతో వల...

క్రెడిట్, డెబిట్ కార్డులు కలిగిన వారికి ఫోన్ చేసి జమ్‌తార నేరగాళ్ళు ముందుగా ఫోన్ రిసీవ్‌చేసుకున్న వ్యక్తిపేరు, ఏ బ్యాంకు కార్డు వినియోగిస్తున్నారో చెప్పి, బ్యాంకు ఉద్యోగులుగా పరిచయం చేసుకుంటూ డెబిట్‌కార్డును ఆధార్‌తో లింక్ చేయాలనో, క్రెడిట్‌కార్డు వివరాలు అప్‌డేట్ చేయాలనో చెప్తుంటారు.

సాధారణంగా ఆయా బ్యాంకులు జారీచేసే కార్డులకు చెందిన సెంటర్లలో మొదటి నాలుగైదు అంకెలు ఒకే సిరీస్‌వి ఉంటాయి.

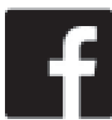
వీటిని ముందుగా చెప్పి మాయగాళ్ళు మిగతా అంకెలు అడుగుతారు.

ఆపై సీ.వి.వి. కోడ్ కూడా తెలిసికొని... కొద్ది సేపటిలో మీకు ఒక వన్‌టైమ్ పాస్‌వర్డ్ వస్తుందని చెప్పి, అది చెప్పితే లింకేజ్, అప్‌గ్రేడ్ పూర్తి అవుతుందని నమ్మిస్తారు.

ఇలా అన్ని వివరాలు తెలుసుకున్న తరువాత వారి ఖాతాలోని నగదును తమ ఖాతాలోకి మార్చుకోవడం, ఆన్‌లైన్‌లో కొనుగోళ్ళు చేయడం చేస్తూ టోకరా వేస్తున్నారు.

కొన్ని సందర్భాలలో ఈ డేటా ఆధారంగా క్లోన్డ్ క్రెడిట్ కార్డులు, డెబిట్ కార్డులు సహితం తయారు చేసి డబ్బులు డ్రా చేసుకుంటున్నారని వెలుగులోనికి వచ్చింది.

వీరు వినియోగిస్తున్న బ్యాంకు ఖాతాలన్నీ తప్పుడు వివరాలతో ఉంటున్నాయని సైబర్ క్రైమ్ అధికారులు చెబుతున్నారు.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

Chittoor Police 9440900005

17. రాజకీయనేతలు, హీరోల ఫోటోలతో ఆన్‌లైన్ ఓటింగ్ పేరుతో మోసం

ఇంటర్నెట్ లింకులు అంటే గుట్టును చేతులు మార్చేస్తున్నాయి. అభిమాన హీరోలకు, రాజకీయ నాయకులకు ఆన్‌లైన్‌లో వేస్తున్న ఓట్లు “ఆర్థిక” పోటుగా మారుతోంది.

ఆర్థిక దోపిడీకి అనువుగా ఉన్న అన్ని మార్గాలను ఉపయోగించుకుంటున్న సైబర్ నేరగాళ్ళు ఇప్పుడు యాప్‌లు, లింకుల ద్వారా సమస్త సమాచారాన్ని లాగేస్తున్నారు.

ఇందుకోసం ప్రత్యేకంగా ప్రోగ్రామ్‌లను రూపొందించుకుంటున్నారు. ఓటీపిలు తెలుసుకొని లక్షలాది రూపాయల ప్రజాధనాన్ని దోచుకుంటున్నారు.

సైబర్ నేరగాళ్ళు సరిక్రొత్త సూత్రాలతో రకరకాల లింక్‌లను తయారు చేస్తున్నారు. ఇఫ్ యు వాంట్ యువర్ ఫేవరెట్ సాంగ్ అని కాప్షన్ పెట్టి లింకులను మెసేజ్ రూపంలో పంపుతున్నారు.

ఆ లింక్ మొత్తం నాలుగైదు దశల్లో ఉంటుంది.

లింక్‌పై ప్రెస్ చేయగానే ఒక పేజీ తెరుచుకొని నెక్స్ట్ అని చూపిస్తోంది. దానిపై క్లిక్ చేయగానే మరో స్టెప్ వస్తుంది.

ఇలా నాలుగైదు స్టెప్స్ దాటినా ఇష్టమైన పాట మాత్రం డౌన్‌లోడ్ కాదు. ఆండ్రాయిడ్ ఫోన్లు ఉపయోగించే వాళ్ళంతా ఇక్కడే పప్పులో కాలేస్తున్నారు.

లింక్ పనిచేయడంలేదనో, సాంగ్ డౌన్‌లోడ్ కాలేదనో వదిలేస్తారు. అసలు మోసం ఇక్కడే ఉన్నది.

లింక్ తెరచుకున్న తరువాత కనిపించే నాలుగైదు దశల్లోనూ ఒక ప్రోగ్రామ్ ఉంటుంది. ఇదంతా హ్యాకింగ్‌కు సంబంధించినదే. ప్రతి పేజీలో ఉన్న హ్యాకింగ్ ప్రోగ్రామ్ దశలవారీగా ఆండ్రాయిడ్ ఫోన్‌లో డౌన్‌లోడ్ అవుతుంది.

ఆ తరువాత మొబైల్ ద్వారా వివిధ యాప్‌లను ఉపయోగించి చేసే ఆన్‌లైన్ షాపింగ్‌తోపాటు ఇతర వివరాలన్నీ సైబర్ నేరగాళ్ళ చేతుల్లోకి వెళ్తాయి.

మనం పంపే మెసేజ్‌లు, సంభాషణల వివరాలన్నీ వారికి తెలుస్తాయి.

ఫేస్‌బుక్ వేదికగా మోసం :

ఫేస్‌బుక్‌లో లైక్‌లకు మహాక్రేజ్ పెరిగింది.

ఉదయం లేచింది మొదలు మనం చేసిన పోస్టులకు లైక్‌లు వచ్చాయో లేదా అని చూసుకోనిదే మరోపని చేయడం లేదు ఫేస్‌బుక్ యూజర్లు.

ఇప్పుడు ఫేస్‌బుక్ వేదికగా ఆన్‌లైన్ ఓటింగ్ నడుస్తోంది.

సినిమా హీరోలు, రాజకీయ నాయకులు, ప్రముఖ క్రీడాకారుల ఫోటోలతో ఫేస్‌బుక్ పోస్టులను ఇంటర్నెట్‌లోకి వదులుతున్నారు.

మీకు నచ్చిన అభిమాని హీరో, రాజకీయ నేత, క్రీడాకారునికి ఓటింగ్ చేయమని ట్యాగ్‌లైన్ పెడుతున్నారు.

దీనిపై క్లిక్ చేసిన తరువాత తెరచుకున్న పేజీ ద్వారా హ్యాకింగ్ ప్రోగ్రామ్ మొబైల్, సెల్‌ఫోన్‌లో డౌన్‌లోడ్ అవుతుంది.

ఎండ్ టు ఎండ్ సెక్యూరిటీ చాలా ముఖ్యం :

సైబర్ నేరగాళ్ళంతా సాంకేతిక నైపుణ్యం ఉన్నవాళ్ళే. ప్రతి నేరానికి ఒక సూత్రాన్ని ఉపయోగించి ప్రోగ్రామ్ తయారు చేసుకుంటారు.

ఎండ్ టు ఎండ్ సెక్యూరిటీ ప్రస్తుత పరిస్థితుల్లో చాలా అవసరం. ఇదివరకు లాటరీ తగిలించి మెసేజ్‌లు వచ్చేవి. ఇప్పుడు ఈ తరచూ మెసేజ్‌లు రావడంలేదు. అంటే సైబర్ నేరగాళ్ళు ట్రెండ్‌ను మార్చారు.

ఈ-మెయిల్‌లోనే కాదు ఆండ్రాయిడ్ మొబైల్ ఫోన్లను హ్యాక్ చేస్తున్నారు. ఇందుకోసం ప్రత్యేక యాప్‌లను రూపొందించి ఇంటర్నెట్‌లోకి వదులుతున్నారు.

ఫోన్లలో ఉన్న యాప్‌లను ప్రతిరోజు అప్‌డేట్ చేసుకోవడం ద్వారా మన సమాచారాన్ని భద్రంగా ఉంచుకోవచ్చు. మనకి తెలియని లింక్ మెసేజ్ వచ్చినా, ఈ-మెయిల్ వచ్చినా వెంటనే డెలీట్ చేయడం మంచిది.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

Chittoor Police 9440900005

18. డిజిటల్ వరీకరణ

యాప్ ద్వారా ర్యాట్ వైరస్ పంపి ఫోను ఆధీనంలోకి...

ప్రస్తుతం అందరి చేతిలో స్మార్ట్‌ఫోన్ ఉంది.

మెసేజ్ నుంచి మనీ ట్రాన్సాక్షన్ వరకు, పెన్ను నుంచి ఫ్లైట్ టికెట్ వరకు అన్ని పనులకు దాదాపు యాప్‌లనే వాడుతున్నారు.

దీనితో కనిపించే యాప్‌లన్నీ డౌన్‌లోడ్ చేసేసుకుంటున్నారు. అయితే కనిపించేవన్నీ యాప్ కాదని తెలుసుకొనేలోపు జరగాల్సిన నష్టం జరిగి పోతుంది.

సైబర్ నేరగాళ్ళు యాప్ లింకులతో ర్యాట్ అనే వైరస్‌ని పంపి మనకు తెలియ కుండానే ఫోన్‌ను ఆధీనంలోకి తీసుకుంటున్నారు.

యాప్స్ ఎంపికలో జాగ్రత్త వహించకుంటే భారీమూల్యం చెల్లించక తప్పదు.

పెన్ను నుంచి పన్నుకట్టే వరకు తమకు కావాల్సిన అన్ని పనులకు అన్ని పనులకు దాదాపు యాప్‌లనే వాడుతున్నారు.

ఇలాంటివారిని దోచుకునేందుకు ఇప్పుడు నేరగాళ్ళు యాప్స్‌నే ఎరగా వేస్తున్నారు.

ఫలానా యాప్ డౌన్‌లోడ్ చేసుకుంటే పాయింట్లు వస్తాయని, ఫ్రీ షాపింగ్ కూపన్లు అంటూ ఓ మెసేజ్‌ను ఫోనుకు పంపిస్తారు.

వీటితో అవసరం ఉన్నా, లేకున్నా ఉచితం కదా అని స్మార్ట్ ఫోన్ వినియోగదారులంతా వీటిని డౌన్‌లోడ్ చేసుకుంటే సైబర్ నేరగాళ్ళ వలలో చిక్కుకోవడం తథ్యమని నిపుణులు హెచ్చరిస్తున్నారు.

తాజాగా గుర్తించిన ఈ తరహా అందోళనకర అంశాన్ని "రిమోట్ అడ్మినిస్ట్రేషన్ ట్రోజన్" (RAT) అని పిలుస్తున్నారు. షార్ట్‌కట్‌లో ర్యాట్ అన్నమాట.

వివిధ రకాల యాప్స్ మాటున నేరగాళ్ళు ప్రత్యేక సాఫ్ట్‌వేర్‌ను గాడ్జెట్స్‌లోనికి జొప్పించి దాని డౌన్‌లోడ్ చేసుకున్న వారి సెల్‌ఫోన్‌లను తమ ఆధీనంలోకి తీసుకుంటున్నట్లు పోలీసులు గుర్తించారు. ఈ తరహా మోసాలపై జాగ్రత్తగా ఉండాలని సైబర్ క్రైమ్ పోలీసులు హెచ్చరిస్తున్నారు.

మన ప్రమేయం లేకుండానే :

మన ప్రమేయం లేకుండానే నేరగాళ్ళ ఆధీనంలోనికి ఫోన్ వెళ్ళిపోవడంతో మనం ఫోన్‌లో చేసే ప్రతి చర్యను అతడు కూడా పర్యవేక్షిస్తుంటాడు. కాల్స్, డేటా వినియోగం, మెసేజ్‌లు, ఫోటోలు, వీడియోలు ఇలా మొబైల్‌లో ఉన్న మొత్తం సమాచారం దాని ఫ్రంట్, బ్యాక్ కెమరాలను సహితం సైబర్ నేరస్తుడు ఈ ర్యాట్ చొప్పించడం ద్వారా తన నియంత్రణలోకి తీసుకోగలడు.

చిన్న మెసేజ్‌తో ప్రారంభమై :

మెసేజ్‌లతో పాటు ఇటీవల సినిమా టిక్కెట్లనుంచి చాలా రకాల బిల్లుల చెల్లింపులను కూడా ఆన్‌లైన్‌లోనే చేసేస్తున్నారు.

తాము ఉచితంగా అందిస్తున్న యాప్‌లో ఆకర్షణలు ఉన్నాయంటూ నేరగాళ్ళు తొలుత బల్క్ మెసేజ్‌లను అనేకమందికి పంపిస్తారు. ఆ ప్రకటనను చూసి ఆకర్షితులైనవారు ఎవరైనా అందులో ఉన్న లింక్‌ను క్లిక్‌చేస్తే చాలు. ఆ యాప్ స్మార్ట్‌ఫోన్‌లోనికి డౌన్‌లోడ్ అవుతుంది.

యాప్‌తోపాటు నేరగాళ్ళు పంపించే ట్రోజన్ కూడా అదే గాడ్జెట్‌లోనికి డౌన్‌లోడ్ అయిపోతుంది. అలా జరిగిన మరుక్షణం నుంచి మన ఫోన్ సైబర్ నేరస్తుడి ఆధీనంలోకి వెళ్ళిపోతుంది.

దూరంగా ఉన్న ఓ వ్యక్తి మన దగ్గరున్న స్మార్ట్ మొబైల్‌ను నియంత్రిస్తూ తనకు అవసరమైన విధంగా వాడుకుంటారు. అందుకే ఈ వైరస్‌ను రిమోట్ అడ్మినేస్ట్రషన్ ట్రోజన్ అని పిలుస్తారు.

సైబర్ నేరగాళ్ళు ఓటిపిని తెలుసుకోవడానికి యాప్‌ద్వారానే ఏర్పాట్లు చేసుకుంటున్నారు. బ్యాంకుల నుంచి వచ్చే ఓటిపిలు ఈ యాప్‌నుంచే వారికి వెళ్ళిపోతాయి. కార్డుల వివరాలు వారివద్ద అప్పటికే సిద్ధంగా ఉంటాయి.

దీనితో ఓటిపి రాగానే వారు తేలికగా లావాదేవీని పూర్తి చేసేస్తున్నారు. ఇలానే సైబర్ నేరగాళ్ళు మనకు తెలియకుండానే దోపిడీలకు తెగబడుతున్నారు.

ఓటిపి అవసరమైన లావాదేవీలను మాత్రం సైబర్ నేరగాళ్ళు అర్థరాత్రి దాటిన తరువాత చేస్తున్నట్లు పోలీసులు గుర్తించారు.

ఆ సమయంలో స్మార్ట్‌ఫోన్ వినియోగదారులు నిద్రలో ఉంటారని, ఈ నేపథ్యంలోనే అతడి ఫోన్‌ను అతని ప్రమేయం లేకుండానే ఓటిపి వచ్చిన విషయమే గుర్తించరని వివరిస్తున్నారు. ఉదయము లేచి జరిగింది తెలుసుకునే సరికి జరగాల్సిన నష్టం జరిగిపోతుంది.

ఇలాంటి అక్రమ లావాదేవీలను చేసే సైబర్ నేరస్తులు ఎక్కువగా బోగస్ వివరాలతో తెరచిన బ్యాంక్ ఖాతాలను వినియోగిస్తున్నారు.

ఆన్‌లైన్‌లో ఖరీదుచేసే వస్తువులను బోగస్ చిరునామాల్లో తీసుకుంటున్నట్లు గుర్తించారు. దీని వలన జరిగిన నష్టంపై ఫిర్యాదులు వచ్చినా వీరిని పట్టుకోవడం సాధ్యం కావడం లేదు.

సరియైన గుర్తింపులేని సంస్థలు, వ్యక్తులు రూపొందించే యాప్స్‌కు దూరంగా ఉండటమే నివారణోపాయమని నిపుణులు సూచిస్తున్నారు.

Chittoor Police 9440900005

19. పెట్టుబడులు పెడతామంటూ ఫేస్‌బుక్ ద్వారా గాలం

మా వద్ద రెండు లక్షల అమెరికన్ డాలర్లు ఉన్నాయి. మీకు పెట్టుబడిగా ఆ డబ్బును సమకూరుస్తాం... మీరు ఏదైనా వ్యాపారం మొదలుపెట్టండి. లాభాల్లో మీకు వాటా ఇస్తాం అంటూ ఓ రిటైర్డ్ ఎస్.బి.ఐ. ఉద్యోగికి కొద్ది నెలల క్రితం అమెరికాకు చెందిన మైఖేల్ ఎస్తేర్ డోనాల్డ్ అనే మహిళ నుండి ఫేస్‌బుక్ వీడియోకాల్ వచ్చింది.

తన వద్ద రెండు లక్షల అమెరికన్ డాలర్లు ఉన్నాయని, మీకు వ్యాపారాల్లో పెట్టుబడులు పెట్టేందుకు వినియోగించుకోవచ్చని నమ్మబలికింది. దీనితో సత్యప్రసాద్ ఆమెతో పలు ధపాలు డాలర్ల విషయమై ఫేస్‌బుక్ ద్వారా ఛాటింగ్ చేయడం, మాట్లాడటం జరిగింది.

ఆ తరువాత అతనితో ఆమెరికాకు చెందిన మాథ్యులేటర్‌తో పాటు, అజయ్ అనే మరోవ్యక్తి కూడా ఫోన్‌ద్వారా పరిచయము అయినారు. వారు ముగ్గురు కలిసి మీకు డబ్బులు పంపిస్తాము కానీ పెట్టుబడులు పెట్టే నిమిత్తం కొంత డబ్బు పన్ను రూపేణ చెల్లించాల్సి ఉంటుందని ఆమె చెప్పింది. అకౌంట్ నెంబరు కూడా ఇచ్చింది. అన్నింటికీ అంగీకరించిన ఆ ఉద్యోగి పలు దఫాలుగా ఆమెకు 28 లక్షల రూపాయలు చెల్లించినాడు. ఆ తరువాత వారి నుంచి ఎటువంటి ఫోన్ రాకపోవడం, ఫేస్‌బుక్ నుంచి కూడా ఛాటింగ్‌లు నిలిచిపోవడంతో అత్యాశకుపోయి మోసపోయినానని అనుకున్నాడు.

20. పోర్న్‌సైట్స్ తెరిస్తే హ్యాక్‌చేసి సిస్టమ్‌లోకి దూరిపోయి బ్లాక్‌మెయిల్

బెంగుళూరుకు చెందిన ఒక సాఫ్ట్‌వేర్ ఇంజనీర్ ఖాళీ సమయంలో నెట్‌లో పోర్న్ సైట్లు చూడటం అలవాటు. ఒకసారి అతనికి ఒక ఈ–మెయిల్ వచ్చింది. అందులోని వార్నింగ్ చూసి ముచ్చెమటలు పట్టాయి? పోలీసులను ఆశ్రయించాడు. ఇంతకీ ఆ ఈ–మెయిల్‌లో ఏమున్నది? నెట్‌లో పోర్న్ దృశ్యాలు చూస్తున్న సమయములో అతని కంప్యూటర్‌లోకి హ్యాకర్ ప్రవేశించాడు. వెబ్ కెమెరాను తన అధీనములోనికి తీసుకున్నాడు. అతని కాంటాక్ట్ లిస్టును హ్యాక్ చేశాడు.

అతనికి తెలియకుండానే వెబ్ కెమరా సహాయంతో అతని వ్యక్తిగత దృశ్యాలను రికార్డ్ చేశాడు. దాని ఆధారముగా ఒక సెక్స్‌టేప్‌ను సిద్ధం చేశాడు. ఈ విషయాన్ని ప్రసావిస్తూ 2200 డాలర్ల విలువగల బిట్ కాయిన్లను చెల్లించు లేదంటే నీ కాంటాక్ట్ లిస్టులో ఉన్నవారికి, కుటుంబ సభ్యులకు ఈ సెక్స్ వీడియోను పంపుతాను అని బెదిరించాడు.

ఇదొక ఫేక్ ఈ–మెయిల్‌గా భావించిన వ్యక్తి ఎందుకైనా మంచిదని కంప్యూటర్‌లోని పర్సనల్ విషయాలు భద్రంగా ఉన్నాయో లేవో అని చూసుకున్నాడు. తొమ్మిది సోర్సులనుంచి తన కాంటాక్ట్స్ హ్యాక్ అయ్యాయని తెలుసుకొని ఖంగుతిన్నాడు. అయితే పరువు పోతుందని బయటకు చెప్పుకోలేక హ్యాకర్లు అడిగినది ఇచ్చుకొని నాలుగు గోడలమధ్య కుమిలి పోతున్నవారు ఉన్నారు. హ్యాకర్లు ఎక్కువగా పోర్న్ సైట్ల ద్వారానే మన ఫోన్లు, కంపూటర్లలోకి ప్రవేశిస్తున్నారు. మనం వారి బెదిరింపులకు లొంగకపోతే రహస్యంగా రికార్డు చేసిన దృశ్యాల తాలూకూ స్క్రీన్‌షాట్‌లు పంపుతున్నారు.

కాబట్టి పోర్న్ సైట్లు చూసే బలహీనతను మానుకోండి :

హ్యాకర్లు బ్లాక్‌మెయిల్ తప్ప మరొ అజెండా ఉండదు. మరి వారు మన వ్యక్తిగత దృశ్యాలను రికార్డు చేశారా అంటే... చేయలేదని మాత్రం ఖచ్చితంగా చెప్పలేము. అయితే మనిషి బలహీనతలను దృష్టిలో పెట్టుకొని మైండ్‌గేమ్ అడేవారు ఉంటారు. అందుకే ధైర్యంగా ఫిర్యాదు చేయాలని సూచిస్తున్నారు పోలీసులు.

21. ప్రేమ చిత్రాలను సోషల్ మీడియాలో పెడతామంటూ బ్లాక్‌మెయిల్

స్నేహంగా మెలిగినప్పుడు యువతీయువకులు చరవాణిలో సరదాగా తీసుకున్న చిత్రాలే... తరువాతి కాలంలో కాలనాగులై కాటేస్తున్నాయి. వారిద్దరి మధ్య బంధం ఏమాత్రం బెడిసికొట్టినా ఆ చిత్రాలే బ్లాక్‌మెయిలింగ్‌కు బాటలు వేస్తున్నాయి. ఆ చిత్రాలను సామాజిక మాధ్యమాలలో అప్‌లోడ్‌చేసి పరువు తీస్తామంటూ బెదిరించేందుకు యువకుల చేతిలో అస్త్రాలు అవుతున్నాయి. ఆ బెదిరింపులు శ్రుతిమించితే ఠాణాల్లో కేసులై... ఆ బెదిరింపు రాయుళ్ళ భవిష్యత్తుకు మచ్చ తెచ్చేందుకు కారణమవుతున్నాయి. ఓ యువతి ఆసుపత్రిలో పనిచేస్తున్నది. అక్కడ ఓ యువకుడితో ఏర్పడిన పరిచయం స్నేహంగా మారింది. కొంతకాలం తరువాత ఆ యువకుడి వైఖరి నచ్చక అతడిని దూరం పెట్టినది. అయితే స్నేహంగా ఉన్నప్పుడు అతనితో కలిసి చిత్రాలు తీసుకోవడమే ఆమె చేసిన తప్పిదముగా మారింది.

ఆ అమ్మాయి తనతో మాట్లాడటం లేదని కక్ష పెంచుకున్న యువకుడు బెదిరింపుల పర్వానికి తెరతీశాడు. నిన్ను ప్రేమించాను, కలిసి తిరిగినప్పుడు నీ కోసం లక్షల్లో ఖర్చు చేశాను. ఇప్పుడు నన్ను దూరం పెడుతున్నావు. అలాంటప్పుడు నేను పెట్టిన ఖర్చులు తిరిగి ఇచ్చేయి, లేదంటే నాతో కలిసిదిగిన ఫోటోలను ఫేస్‌బుక్‌లో పెట్టి పరువుతీస్తా... అంటూ హెచ్చరిక సందేశాలు పంపించడం ఆరంభించాడు. ఎకంగా రూ. 3.50 లక్షలు ఇవ్వాలని బెదిరిస్తూ ఉండటంతో బెంబేలెత్తిన బాధితురాలు పోలీసుల్ని ఆశ్రయించింది. కేసు నమోదు చేసిన పోలీసులు దర్యాప్తు ప్రారంభించారు.

ఫేస్‌బుక్ పరిచయం... వేదింపు పర్వం :

ఓ మహిళకు కొన్ని సంవత్సరాల మునుపు పెళ్ళి అయినది. భర్తతో కలిసి ముంబయిలో

ఉంటున్నది. ఆమెకు కొంతకాలం క్రితం ఫేస్‌బుక్‌లో మరో యువకునితో పరిచయం ఏర్పడినది. ఆమె హైదరాబాద్‌కు వచ్చినప్పుడు అతడు వెళ్ళి కలిసినాడు. స్నేహంగా ఉంటాడనుకున్న ఆ యువకుడు శ్రుతిమించి ప్రవర్తిస్తుండటం ఆమెకు నచ్చలేదు. అతనితో ఛాటింగ్ మేనేసింది.

అయితే అతను మాత్రం ముంబయి వెళ్ళి ఆమెను కలిసే ప్రయత్నం చేశాడు. బాధితురాలు విషయాన్ని తన భర్తకు చెప్పింది. ఆగ్రహించిన ఆమె భర్త ఆ యువకునికి దేహశుద్ధి చేసి పంపిచినాడు.

అంతటితో ఆ యువకునిలోని మరోకోణం బయటికివచ్చింది. అన్ని రోజులు తనతో స్నేహంగా ఉండి కొట్టించిదనే కోపంతో బ్లాక్‌మెయిలింగ్‌కు దిగాడు. 50 లక్షల రూపాయలు ఇవ్వాలంటూ బెదిరించడం ఆరంభించాడు. లేదంటే హైదరాబాద్‌కు వచ్చినప్పుడు తీసిన ఆమె చిత్రాలను ఫేస్‌బుక్‌లో అప్‌లోడ్ చేస్తానంటూ హెచ్చరించడం మొదలుపెట్టాడు. హెచ్చరికలు తీవ్రరూపం దాల్చడంతో బాధితురాలు ఆ విషయాన్ని తండ్రికి చెప్పింది. ఆమె తండ్రి కె.పి. హెచ్.బి. పోలీసులకు ఫిర్యాదు చేయడంతో ఆ యువకునికోసం వేట మొదలైనది.

మల్కాజ్‌గిరికి చెందిన ఒక వ్యక్తి నకిలీ ఫేస్‌బుక్ యూజర్ ఐడి "వర డార్లింగ్"ను సృష్టించి అమ్మాయిలకు ఫ్రెండ్ రిక్వెస్ట్‌ను పంపేవాడు. ప్రొఫైల్‌లో అమ్మాయిగా భావించి పలువురు యువతులు ఆమెదించారు.

ఆ తరువాత అతను వీడియో ఛాటింగ్‌కు రావాలని, నగ్నంగా కనిపించాలని కోరేవాడు. ఈ ప్రతిపాదన తిరస్కరించిన అమ్మాయిల ముఖాన్ని మార్ఫింగ్‌చేసి బాధితుల ఫేస్‌బుక్ మెసెంజర్‌కు పంపేవాడు.

తన మెసేజ్‌లకు స్పందించకపోతే ఆ ఫోటోలను ఫేస్‌బుక్ ఫ్రెండ్స్‌తో పాటు పోర్న్ వెబ్‌సైట్‌లలో అప్‌లోడ్ చేస్తానని బెదిరించడంతో బాధితురాలు రాచకొండ సైబర్‌క్రైమ్ పోలీసులను ఆశ్రయించినది.

ఇలాంటి ఘటనలు కేవలం ఒకరు, ఇద్దరు యువతులకే పరిమితం కావడంలేదు. వందల సంఖ్యలో విద్యార్థినులు, యువతులు, మహిళలు ఇదే తరహాలో వేదింపులు ఎదుర్కొంటున్నారు. ఫేస్‌బుక్, యూట్యూబ్‌లలో తమ చిత్రాలు, వీడియోలను అప్‌లోడ్ చేస్తున్నారని పోలీసులను ఆశ్రయిస్తున్నారు. వీటిని విశ్లేషించిన పోలీస్ అధికారులు అపరిచితులు పంపిన చిత్రాలు, పోస్ట్‌లకు స్పందించవద్దని సూచిస్తున్నారు.

ఫేస్‌బుక్ ఖాతాలతో జరభద్రం :

ఫేస్‌బుక్ ఖాతాలతోనే విద్యార్థినులు, యువతులు, మహిళలకు ప్రమాదాలు పొంచి ఉన్నాయని సైబర్ క్రైమ్ అధికారులు పేర్కొంటున్నారు. గుర్తుతెలియని వ్యక్తులు పంపిన చిత్రాలు, డాక్యుమెంట్‌కు లైక్ కొట్టడం ప్రమాదాలను కొని తెచ్చుకోవడమేనన్నారు. స్నేహితులతో గడిపిన సందర్భాలు, దేవాలయాలు, సినిమా థియేటర్లు, హోటళ్ళు, విహార యాత్రలు, పెళ్ళిళ్ళ సమయంలో తీసుకున్న ఫోటోలను ఫేస్‌బుక్‌లో పోస్టు చేయడంతో సైబర్ నేరగాళ్ళు వీటిని దుర్వినియోగం చేస్తున్నారు.

ఫేస్‌బుక్ అకౌంట్‌లోకి వస్తున్న నేరగాళ్ళు ముఖ్యముగా యువతులు, విద్యార్థినులు లక్ష్యంగా చేసుకొని వేధింపులు, బెదిరింపులకు పాల్పడుతూ హెచ్చరికలు చేస్తున్నారు. నిందితులలో బాధితులకు తెలిసినవారు కూడా ఉండటం గమనార్హం.

ఫేస్‌బుక్, ట్విటర్‌లలో ఖాతాలున్న యువతులు, విద్యార్థినుల వ్యక్తిగత వివరాలు, ఒంటరిగా ఉన్నప్పుడు తీసుకున్న ఫోటోలు, వీడియోలను నేరగాళ్ళు డౌన్‌లోడ్ చేసుకుంటున్నారు. తమ చిత్రాలను అసభ్యకరంగా మార్చి ఫేస్‌బుక్‌లో ఉంచుతున్నారని సైబర్‌క్రైమ్ పోలీసు ఠాణాలకు వస్తున్న బాధితుల సంఖ్య రోజురోజుకు పెరుగుతోంది.

బ్లాక్ మెయిలింగ్, డబ్బులు డిమాండ్ :

యువతులు, విద్యార్థినులు ఒంటరిగా ఉన్నప్పుడు తీసుకున్న ఫోటోలను అప్‌లోడ్ చేస్తుండటం కూడా తలనొప్పి తెచ్చిపెడుతోంది. ఈ ఫోటోలను డౌన్‌లోడ్ చేస్తున్న నిందితులు ఫేస్‌బుక్ ద్వారా వారితోనే ఛాట్‌చేస్తూ ప్రేమ పేరుతో వలవేస్తున్నారు. దారిలోనికి రాకుంటే వారి వ్యక్తిగత ఫోటోలను మార్ఫింగ్ చేసి సోషల్ మీడియాలో పెడుతున్నారు.

గతంలో ఒక బి.టెక్. విద్యార్థి ఇంటర్నేషనల్ స్కూలు చెందిన విద్యార్థులతో ఫేస్‌బుక్‌లో అమ్మాయిగా పరిచయం చేసుకొని వ్యక్తిగత వివరాలు సేకరించి వేధింపులకు గురిచేశాడు.

కొందరి నుంచి డబ్బులు డిమాండ్‌చేసి తన ఖాతాల్లో జమ చేయించుకున్నాడు. చివరకు ఓ విద్యార్థిని ధైర్యంచేసి తన తల్లితండ్రులకు చెప్పడంతో అతని అగడాలకు అడ్డుకట్ట పడింది.

ఎవరైనా వేధింపులు తీవ్రమైనప్పుడు మాత్రమే తల్లితండ్రుల దృష్టికి తీసుకెళ్ళుతున్నారు. అదే అదనుగా భావిస్తున్న సైబర్ నేరగాళ్ళు బ్లాక్‌మెయిల్ చేసి బాధితుల నుంచి డబ్బు తీసుకునేందుకు ఫేస్‌బుక్‌ను వేదికగా వాడుకుంటున్నారు.

వ్యక్తిగత చిత్రాలు, వీడియోలు వద్దు :

ఫేస్‌బుక్‌లో నిక్షిప్తంచేసిన వ్యక్తిగత ఫోటోలు, వీడియోలు మార్ఫింగ్ చేసి వేధింపులకు గురిచేస్తున్న నేరగాళ్ళ సంఖ్య పెరుగుతోంది. అమ్మాయిలు ఫేస్‌బుక్‌లో తెలియనివారి నుంచి వచ్చిన ఫ్రెండ్ రిక్వెస్ట్‌లను ఎట్టి పరిస్థితులలో యాక్సెస్ చేయవద్దు. అమ్మాయే కదా అని స్పందిస్తే ఆ తరువాత వ్యక్తిగత వివరాలు తెలుసుకోవడంతో పాటూ ఫోటోలను సేకరించి బ్లాక్‌మెయిల్ చేస్తున్నారు. కొందరు శారీరకంగా లొంగతీసుకునేందుకు ఎత్తులు వేస్తున్నారు. మరికొందరు డబ్బులకోసం ఈ మార్గాన్ని ఎంచుకుంటున్నారు. వీటన్నింటినీ దృష్టిలో పెట్టుకొని అమ్మాయిలు అన్ని విషయాలలో జాగ్రత్తగా వ్యవహరించాలి.

ఓ కాలేజీలో బీ.టెక్. చదువుతున్న ఓ విద్యార్థి అదే కాలేజీలో స్నేహితుడు మరో బ్రాంచీలో విద్యనభ్యసిస్తున్నాడు. అతను ఓ రోజు తన క్లాస్‌రూమ్‌లో అస్వస్థతకు గురి అయినాడు. దీనితో అతడు అతడు అక్కడకు వెళ్ళి సపర్యలు చేయడానికి సిద్ధపడ్డాడు. అయితే దీనికి ప్రొఫెసర్ అభ్యంతరం చెప్పడంతోపాటు ఓ విద్యార్థినితో వాగ్వాదం జరిగింది. ఆమెపై కక్ష కట్టిన ఆ విద్యార్థిని ఫేస్‌బుక్‌లో ఉంచిన ఆమె ప్రొఫైల్ చిత్రాన్ని డౌన్‌లోడ్ చేసి దానితోపాటు

ఫోన్ నెంబరును "లోకంటో" అనే అశ్లీల వెబ్‌సైట్‌లో అప్‌లోడ్ చేశాడు. అంతటితో ఆగకుండా అసభ్య మెసేజ్‌లను పోస్ట్ చేశాడు. నాతో సెక్స్‌ఛాట్ చేయాలనుకునే వారు 1,200/-, నగ్న చిత్రాలు కావాలంటే ఒక్కో చిత్రానికి 200/-, శృంగారంలో పాల్గొనాలంటే 5,000/- రూపాయలు చెల్లించాలని చెప్పలేని విధంగా అసభ్యకర మెసేజ్‌లను అప్‌లోడ్ చేశాడు. సెక్స్‌కు సంబంధించిన విషయాలు మాట్లాడాలంటే "కాల్ మీ సెక్సీ బాయ్స్" అంటూ మెసేజ్ పెట్టాడు.

ఓ డిగ్రీ విద్యార్థిని తన స్నేహితురాలి ద్వారా ఓ యువకుడు పరిచయమైనాడు. ఆమె తన సోదరుడిగా పరిచయము చెయ్యడంతోపాటూ అతడు కోరడంతో సెల్ నెంబరు చెప్పింది. అప్పటినుండి మెసేజ్‌లు, కాల్స్‌తో వేధింపులు మొదలయినాయి.

ఆమెకు వివాహము అయినాకూడా బ్లాక్‌మెయిల్ చేస్తున్న అతగాడు 30 లక్షల రూపాయలు డిమాండ్ చేశాడు. బాధితురాలి ఫిర్యాదుతో షీ టీమ్ అతనిని పట్టుకొని స్థానిక పోలీసులకు అప్పగించాయి.

మానసిక క్షోభ :

ఓ ప్రబుద్ధుడు చేసిన పనికి ఆమెకు పగలు, రాత్రి అనే తేడా లేకుండా ఫోన్లు రావడం మొదలయ్యాయి. నీ రేటెంత... ఎక్కడ కలవాలి... ఏ సమయంలో? అంటూ ఆమెతో అసభ్యంగా మాట్లాడడంతో మానసిక క్షోభకు గురిఅయినది. మరికొంతమంది అసభ్యకర మెసేజ్‌లను ఆమెకు వాట్సప్ చేసేవారు. వారి వేధింపులు భరించలేక రాచకొండ క్రైమ్ పోలీసులను ఆశ్రయించి విషయం చెప్పారు.

22. అనధికారిక లింకులను నొక్కితే మీ ఫోను హ్యాకర్ కంట్రోల్ అవుతుంది

స్మార్ట్‌ఫోన్ కొనేస్తాము, ఏ యాప్ దేనికో తెలుసుకుంటాం, ఎడాపెడా వాడేస్తాం మంచిదే! కాని మీ ప్రైవసీ మాటేంటి? మీ ఫోన్ మీ కంట్రోల్‌లోనే ఉందా? ఎవరైనా వశీకరణ మంత్రం వేశారా? వేలు పోసి కొన్న ఫోన్, దానికొక స్క్రీన్‌గార్డు, బ్రాండెడ్ పౌచ్‌లతో భద్రంగా చుసుకుంటాము. ఎక్కడున్నా, ఏమి చేస్తున్నా ఫోన్ వెంట ఉండాల్సిందే. అలాంటప్పుడు నా ఫోన్ నా కంట్రోల్లో లేకుండా ఇంకెవరో కంట్రోల్‌లోకి ఎలా వెళ్తుంది? ఏమి మాట్లాడుతున్నారు? అని స్పందించే మొబైల్ యూజర్లు లేకపోరు. ఎందుకంటే వారికి తెలిసి ఫోన్‌ని సురక్షితంగా వాడడమంటే క్రిందపడకూడదు, దుమ్ము చేరకూడదు, గీతలు పడకూడదు. ఇవి సరే.... ఫోన్‌లోని సమాచార గోప్యత సంగతేంటి? ఇప్పుడిప్పుడే డిజిటల్ ఇండియాకి అప్‌డేట్ అవుతున్న వారంతా ఖచ్చితంగా ఆలోచించాల్సిన విషయం. ఎందుకంటే హ్యాకర్ల డిజిటల్ వశీకరణకు మీ ఫోన్ చిక్కడం తథ్యం. తస్మాత్ జాగ్రత్త.

- సార్, ఒక్క నిమిషం మీ ఫోన్ ఇస్తారా? ఇంట్లో ఫోన్ మర్చిపోయా? అర్జెంట్‌గా ఒక కాల్ చేయాలి అంటూ వినయంగా అడుగుతారు. 'మరేం పర్వాలేదు' తీసుకోండి అని

మనం అతనికి ఫోన్ ఇచ్చారు. కొంతసేపటి తరువాత 'థ్యాంక్స్ అండీ' అని ఫోన్‌ను తిరిగి ఇచ్చే వెళ్ళిపోతాడు. ఫోన్ తీసుకున్న వ్యక్తి క్షణాల్లో స్పై యాప్‌ని ఫోన్‌లో ఇన్‌స్టాలో చేసి వదిలేస్తాడు.

- ఫోన్‌ను ఎక్కడపడితే అక్కడ వదిలేసి పోతుంటారు. ఇంట్లోనేనా? ఆఫీసుల్లో, పార్కుల్లో వెళ్ళిన ప్రతిచోట ఇలాగనే వదిలేస్తుంటారు. ఆ ఫోన్ ఎవరైనా మోసగాని చేతిలో పడితే వదలి వెళ్ళిన ఫోన్‌లో ఓ ఫైల్‌ని వదిలారంతే.
- వాట్సప్ చెక్ చేస్తుంటే 'ఫ్లిప్‌కార్ట్‌లో బంపర్ ఆఫర్, ఐఫోన్ ఎక్స్ రూ. 5,000/- మరిన్ని వివరాలకు లింక్‌ను క్లిక్ చేయండి' అని కనిపించిందో ఫార్వర్డ్ మెసేజ్. ఒక్క క్షణం ఆలోచించకుండా క్లిక్ చేశారు. ఏదో వెబ్‌పేజి ఓపెన్ అయింది. కాసేపు లోడ్‌అయి టైమ్‌అవుట్ ఎర్రర్ మెసేజ్ వచ్చింది. 'ఛా... పూర్ నెట్‌వర్క్‌తో చస్తున్నాం...' అని క్లోజ్ చేసినారు. దీని వలన మీరు మీ చేతులతో మీ లింక్‌ని క్లిక్‌చేసి మీ ప్రైవసీ మొత్తాన్ని తీసుకెళ్ళి హ్యాకర్ చేతిలో పెట్టినారు.

పై మాదిరిగా మీరు హ్యాకర్ల వలకి చిక్కి ఉండవచ్చు. ఫోన్ తళతళ మెరుస్తూనే ఉంటుంది. కానీ మీ మొత్తం సమాచారం హ్యాకర్‌కి చేరిపోతుంది. మీ మాటలు... మీ మెసేజ్‌లు... ఫోటోలు... వీడియోలు... ఇలా ఫోన్ మీదంటూ వ్యక్తిగతం అనుకోవడానికి ఏదీ మిగలదు. వీళ్ళే కాదు... చాలామంది యూజర్లు సైబర్ సెక్యూరిటీపై సరియైన అవగాహన లేక హ్యాకర్ల డిజిటల్ వశీకరణకు బలి అవుతున్నారు.

రెండే నిమిషాలలో... :

ఫోన్ హ్యాకర్ల చేతికి వెళ్ళినా... వారు పంపినా మెసేజ్‌ని క్లిక్ చేసినా... కేవలం 20 సెకన్ల నుంచి 2 నిమిషాలల్లో ఫోన్‌ను వారి కంట్రోల్‌లోకి తీసుకుంటారు. అందుకు వాళ్ళు ఉపయోగించేది 2 యం.బి. సైజ్ ఉన్న చిన్న ఫైల్ మాత్రమే. అదో సాఫ్ట్‌వేర్ అప్లికేషన్ క్లయింట్. రిమోట్ వెర్షన్లతో దీనిని రూపొందిస్తారు. క్లయింట్ వెర్షన్ సాఫ్ట్‌వేర్‌ని ఫోన్‌లో ఇన్‌స్టాల్ చేస్తేచాలు. వశీకరణకు వ్యవస్థ సిద్ధం అయిపోతుంది. ఫైల్‌ని ఓ వెబ్ లింకులా మెసేజ్ రూపంలోనో, వాట్సప్ ఛాట్‌లోనో, ఈ మెయిల్‌లోనో పంపుతారు. దీనిపై క్లిక్‌చేస్తే ఫైల్ డౌన్‌లోడ్ అయి ఇన్‌స్టాల్ అవుతుంది. యాప్స్ రూపంలోనూ ఈ ప్రమాదకరమైన స్పైవేర్‌ని ఫోన్‌లో వెళ్ళేలా ప్రయోగిస్తున్నారు. ఎక్కువగా గేమ్స్, మ్యూజిక్, ఇతర యాప్స్ రూపంలో ఈ ప్రమాదకర ఫైల్స్ ఫోన్‌లోరి ప్రవేశిస్తాయి. అది మొదలు ఎప్పుడంటే అప్పుడు హ్యాకర్ తన డ్యాష్‌బోర్డుపై రిమోట్ వెర్షన్ అప్లికేషన్‌ని వాడుకొని మీకు సంబంధించిన మొత్తం వివరాలను యాక్సెస్ చేస్తాడు.

లొకేషన్ ట్రాకింగ్ : మీరు ఎక్కడున్నారో, ఎటు వెళ్తున్నారో చూడొచ్చు.

కాల్ ట్రాకింగ్ : ఎన్ని కాల్స్ చేశారు, ఏయే నంబర్లనుంచి కాల్స్ వచ్చాయో మొత్తం చిట్టాను విప్పేస్తారు.

ఇన్‌బాక్స్ ట్రాకింగ్ : ఫోన్‌కి వచ్చే మొత్తం టెక్స్ట్ మెసేజ్‌లను చూడొచ్చు. అర్థిక లావాదేవీలకు వాడే ఓటిపిలను తెలుసుకునేందుకు ఇదే సరియైన మార్గము.

కెమరా ట్రాకింగ్ : ఫోన్ కెమెరాతో మీరున్న చోటుని ఫోటోలు తీసి చూడచ్చు. మీరు ఎక్కడ ఉన్నారు? ఎవరితో కలుస్తున్నారో కెమెరా కంటితో చూస్తారు.

మైక్రోఫోన్ ట్రాకింగ్ : ఫోన్‌కి ఉన్న మైక్రోఫోన్‌ని ఆన్‌చేసి మీ సంభాషణల్ని వినొచ్చు. రికార్డు చేయవచ్చును.

వాట్సప్, స్నాప్‌ఛాట్ : సోషల్‌ఛాట్ చిట్టాలను విప్పి అన్నీ చదివేస్తారు.

ఫేస్‌బుక్, ట్విటర్ : ఇటువంటి వేదికల్లోని సోషల్ లైఫ్‌లోకి ఎంటరైపోతారు. దీనితో మీ నెట్‌వర్క్‌లో స్నేహితుల ఆల్బమ్‌లు, వీడియోలు, ఇతర డేటాని యాక్సెస్ చేస్తారు. నెట్‌వర్క్‌లో పంచుకునే ముఖ్యమైన సమాచారంపై ఓ కన్ను వేస్తారు.

ఆసక్తులన్నీ పసికట్టే... :

వ్యక్తి గురించి ముందే ఒక అంచనాకు రావాలంటే? సోషల్ నెట్‌వర్క్ ప్రొఫైల్‌ని చూస్తే చాలు. ఆవలించకుండానే ప్రేగులు లెక్కపెట్టవచ్చును. హ్యాకర్లు కూడా ఇదే చేస్తున్నారు. ముందు యూజర్ల సోషల్ లైఫ్‌ని క్షుణ్ణంగా పరిశీలించి వారి ఆసక్తుల ఆధారంగా వలవేసున్నారు.

మీకు గేమింగ్‌లు ఇష్టమైతే అందుకు సంబంధించిన వివరాలతో ఓ నకిలీ యు.ఆర్.ఎల్‌ని జనరేట్ చేసి పంపిస్తాడు. ఇదేమాదిరి మ్యూజిక్, వింతలు, విశేషాలతోనూ నకిలీ యాప్స్‌ని తయారుచేసి పంపుతారు. ఈ విధానాన్ని సాంకేతికంగా సోషల్ ఇంజనీరింగ్ అంటారు.

ఆండ్రాయిడ్ యూజర్లు ఒక్కసారి 'ఏ.పి.కె.' ఎక్స్‌టెన్షన్ ఫైల్‌ని ఇన్‌స్టాల్ చేసే క్రమములో అన్ని అధికారిక యాప్‌ల మాదిరిగానే అనుమతులు కోరుతుంది. అన్నింటినీ ఓకే చేస్తూ నెక్ట్స్, నెక్ట్స్ నొక్కేస్తూ ఇన్‌స్టాల్ చేస్తాము. ఇంకేముంది... మీ చేత్తో మీరే ప్రైవసీని వేరొకరి చేతిలో పెట్టేస్తారు.

చిక్కకూడదంటే ఖచ్చితంగా కొన్ని నియమాలు పెట్టుకోవాలి :

గుర్తు తెలియని వ్యక్తులు ఫోన్‌కాల్ కోసమో... మరేదైనా అవసరానికి అడిగితే సున్నితంగా తిరస్కరించండి. టీనేజర్లతో ఎక్కువగా ఈ తరమా సైబర్ నేరాలు పెరుగుతున్నాయి. అమ్మాయో, అబ్బాయో ఎవరైనా ఫోన్ అడిగి తీసుకుంటారు. వారి నెంబర్‌కే కాల్‌చేసి తిరిగి ఇచ్చేస్తారు. తరువాత మీ నెంబరుకు యూ.ఆర్. లింకులతో వలేసి పట్టేస్తున్నారు. ఓటిపిలు, బ్యాంకింగ్ వివరాల్ని తెలుసుకొని డబ్బు కాజేయడమో... నెట్టింట్లో షాపింగ్ చేయడమో చేస్తున్నారు. ఒకవేళ మీ ఫోన్‌ని ఇతరులకు ఇవ్వాల్సివస్తే తీసుకున్న తరువాత ఏమైనా యాప్‌లు ఇన్‌స్టాల్ చేశారేమో చెక్ చేయండి. సందేహముగా అనిపిస్తే డేటాను బ్యాకప్ తీసుకుని ఫోన్ 'ఫ్యాక్టరీ రీసెట్' చేయడం మంచది.

ఫోన్ నెంబర్లను అపరిచితులకు ఇవ్వవద్దు. కాస్త నిశితంగా పరిశీలిస్తే షాపింగ్ మాల్స్‌లో లక్కీడ్రాఅనో... మరేదైనా బహుమతులు అనో కూపన్లు ఇస్తారు. దాంట్లో మీ అడ్రస్‌తో పాటు ఫోన్ నెంబర్‌ని వ్రాయమని కోరతారు. మరో ఆలోచన లేకుండా వ్రాసి

ఇస్తాము. పేరొందిన సంస్థలైతే ఆయా వివరాలను గోప్యంగాఉంచుతాయి. కానీ కొన్ని సంస్థలు ఇలా సేకరించిన మొత్తము సమాచారాన్ని డబ్బుకోసం సైబర్ నేరగళ్ళకు అమ్ముకునే అవకాశం లేకపోదు. అందుకే ఉచిత బహుమతులంటూ వివరాలు కోరితే ఇవ్వకపోవడమే మంచిది.

స్మార్ట్‌ఫోన్‌తో పాటు మరొక బేసిక్ ఫోన్‌ని కొని వాడండి. ఓటిపిలు, పాస్‌వర్డ్‌లు, ఇతర బ్యాకింగ్ అవసరాలకు వాడే కాంటాక్ట్ నెంబరును బేసిక్ ఫోన్‌లోనే వాడండి. వ్యక్తిగతమైన, ఇతర కాల్స్, ఫోన్ నెంబర్లు అన్నీ దాంట్లోనే సేవ్ చేసుకుని వాడితే మంచిది. నెట్ సౌకర్యంలేని బేసిక్ ఫోన్‌ని హ్యాక్ చేయడం అసాధ్యం. ఇక స్మార్ట్‌ఫోన్‌లో ఎలాంటి వ్యక్తిగతమైన వివరాలను ఉంచవద్దు. రిజిస్టర్ అయ్యేటప్పుడు కూడా పేర్లు పెట్టుకోండి. యాప్‌లోగానీ, ఏదైనా నెట్టింటి సర్వీసుల్లో నకిలీ డేటాతోనే నమోదైతేనే మంచిది.

నెట్టింట్లో ఆర్థిక లావాదేవీలు చేసే యాప్‌లను నిశితంగా పరిశీలిస్తూ వాడాలి. ఎప్పటికప్పుడు అధికారిక వెబ్‌సైట్ల నుంచి అప్‌డేట్స్ చేస్తుండాలి. బ్యాంక్ అకౌంట్ స్టేట్‌మెంట్లను పరిశీలిస్తూ ఉండాలి. ఇన్‌బాక్స్‌ని ఆటోమెటీక్‌గా యాక్సెస్ చేసే అనుమతుల్ని యాప్‌లకు ఇచ్చియుంటే ఓటిపిలను హ్యాకర్లు యాక్సెస్ చేసే వీలుంటుంది. దీనితో ఆర్థిక లావాదేవీలను ఇతరులు కంట్రోల్ చేయవచ్చు.

ఎక్కువ మొత్తంలో జీతాలు జమ అయ్యే బ్యాంకు ఖాతాలను నెట్ బ్యాంకింగ్‌ను వాడకపోవడమే మంచిది.

విధిగా ఇంటర్నెట్ బ్యాంకింగ్ చేయాల్సివస్తే తక్కువ మొత్తంలో ఎకౌంట్‌కి జమచేసి వాడుకుంటే మేలు. ఉదాహరణకు నెలకు 10,000/- రూపాయలు డబ్బును జమచేసి అదే అకౌంట్ నుంచి ఆన్‌లైన్ లావాదేవీలు చేయడం ఉత్తమం.

గుర్తు తెలియని వ్యక్తుల నుంచి వచ్చే మెయిల్స్‌కి స్పందించవద్దు. ఒక వేళ చూడాలని అనుకుంటే మెయిల్‌లో లింక్‌ని క్లిక్ చేయకుండా కాపీచేసి బ్రౌజర్‌లో పేస్టుచేసి ఓపెన్ చేయండి.

యూ.ఆర్. లింకులతో సోషల్ నెట్‌వర్కుల్లో వచ్చే మెసేజ్‌లను పట్టించుకోవద్దు.

అనధికారంగా యాప్‌స్టోర్‌లో కనిపించిన వాటిని ఇన్‌స్టాల్ చేయకపోవడమే మంచిది.

ఫోన్‌లోని యాంటీవైరస్‌లను ఎప్పటికప్పుడు అప్‌డేట్ చేయడం తప్పనిసరి. నిర్ణీత సమయానికి ఫోన్‌ని స్కాన్ చేసి సమస్యలను చెక్‌పెడితే మంచిది.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

23. యాప్‌లకు పర్మిషన్ ఇచ్చేటప్పుడు జర జాగ్రత్త, మనకు తెలియకుండానే పని చేసే మైక్రో ఫోన్, కెమెరా

వ్యక్తిగత గోప్యత మన ప్రాథమిక హక్కు అని రాజ్యాంగం చెబుతుంది. కానీ... స్మార్ట్ ఫోను వచ్చాకా జీవితాల్లో గోప్యత అనే మాటకు అర్థం లేకుండా పోయింది. మీరెక్కడున్నారనే విషయాన్నీ మీ ఫోనులో లొకేషన్ ఎనేబుల్ చేయడం ద్వారా గుర్తించొచ్చు.

ఆన్‌లైన్‌లో మీరు దేనికోసం వెతికారో ఆ శోధన ఆధారంగా మీకు వాణిజ్య ప్రకటనలు పంపించవచ్చు. ఇదంతా ఎలా సాధ్యమవుతుందంటే... యాప్స్ ఇన్‌స్టాల్ చేసేటప్పుడు మనం ఒక్క క్షణం కూడా ఆలోచించకుండా సదరు యాప్‌లు ఏ పర్మిషన్ అడిగితే ఆ పర్మిషన్ ఇచ్చేయడం వల్లనే. ఉదాహరణకు డిక్షనరీ యాప్‌కు కెమెరాతో, కాంటాక్ట్స్‌తో పనే ఉండదు. కాని వాటిని ఉపయోగించుకునేందుకు అనుమతి కోరుతాయి. మనం అనాలోచితంగా ఇచ్చేస్తాం. ప్రామాణిక సంస్థలు తయారుచేసే యాప్‌లైతే ఇలాంటి అనుచిత అనుమతులు కోరవు.

మెటాస్ప్లోయిట్... ఎథికల్ హ్యాకింగ్ ప్లాట్ ఫాం అయిన ఖాళీలో ఒక అప్లికేషన్ ఇది. ఈ యాప్ ద్వారా ఒక పీడీఎఫ్ ఫైల్‌ను పంపి ఒక వ్యక్తి సమాచారం మొత్తాన్నీ తెలుసుకోవచ్చు. ఆ ఫోన్ వినియోగదారుడికి తెలియకుండా... ఏ స్టాఫ్ వేర్ కావాలంటే ఆ సాఫ్ట్‌వేర్‌ను దాంట్లో ఇన్‌స్టాల్ చేయొచ్చు. కీలాకర్ సాఫ్ట్‌వేర్‌ను నిక్షిప్తం చేసి వారి పాస్వర్డ్‌లన్నింటినీ తెలుసుకోవచ్చు. ఆ ఫోన్‌లో వున్న ప్రతి డాక్యుమెంట్‌ను, ఫోటోను, వీడియోను చూడొచ్చు. వేరొకరికి పంపించవచ్చు. వీడియోలు, ఆడియోలు తీయడం, వేరొకరికి షేర్ చేయడం సరేసరి.

గేమింగ్ యాప్స్‌తో జర భద్రం :

మామూలు యాప్స్‌తో పోలిస్తే గేమింగ్ యాప్‌లు వినియోగదారుల సమాచారాన్ని సేకరించి వాణిజ్య సంస్థలకు అమ్ముకోవడం ఎక్కువ అని సైబర్ భద్రత నిపుణులు చెబుతున్నారు. ఉదాహరణకు... న్యూయార్క్ టైమ్స్ పత్రిక ఇటీవలే 'ఆల్ఫోన్సో' అనే స్టార్టప్ రూపొందించిన సాఫ్ట్‌వేర్‌తో పనిచేసే యాప్స్ గురించి ఒక కథనాన్ని ప్రచురించింది.

ఆ సాఫ్ట్‌వేర్ సాయంతో ఆల్ఫోన్సో సంస్థ.. సదరు యాప్స్‌ను వాడేవారు. ఏయే టీవీ ప్రోగ్రాములు చూస్తున్నారో, వారి బ్రౌజింగ్ అలవాట్లు ఏమిటో ఆ సమాచారం మొత్తాన్నీ సేకరించి అడ్వర్టయిజ్‌మెంట్ సంస్థలకు విక్రయిస్తోందని ఆ కథనం.

ఇంటర్నెట్ చూస్తున్నప్పుడు... మన కంప్యూటర్‌కు అమర్చిన వెబ్ కెమెరానో, మన ఫోన్‌లోని కెమెరానో మన ఫోటోలు తీసి వేరొకరికి పంపిస్తుందని ఊహిస్తామా? 'ఆప్టిక్ నెర్క్' అనే ప్రోగ్రామ్ ద్వారా బ్రిటన్ నిఘా సంస్థ జీ.సీ.హెచ్.క్యూ 18 లక్షల మంది వినియోగదారుల చిత్రాలను సేకరించింది. ప్రతి ఐదు నిమిషాలకొకసారి వారి కంప్యూటర్‌కు అమర్చిన వెబ్ కెమెరానే వారి ఫోటోలను తీసిపంపేది. ఈ విషయాన్ని వికీలీక్స్ వ్యవస్థాపకుడు ఎడ్వర్డ్ స్నోడెన్ బయటపెట్టాడు.

మన బతుకంతా హ్యాకర్ల చేతిలో!

- ఒక యాప్ ఇన్‌స్టాల్ చేసేటప్పుడు కెమెరా, మైక్రోఫోన్ వాడుకోవడానికి మనం అనుమతి ఇచ్చామంటే.. ఆ యాప్ మన ఫోన్‌లోని కెమెరాలనూ యాక్సెస్ చేయగలదు. మన ఫోన్‌లోని మైక్రోఫోన్ ద్వారా మన మాటలను రికార్డు చేయగలదు.
- మనకు తెలియకుండానే మన ఫోటోలు, వీడియోలు తీయగలదు. వాటిని థర్డ్ పార్టీలకు అప్‌లోడ్ చేయగలదు.
- ఒక వాణిజ్య ప్రకటననో, వీడియోనో చూస్తున్నప్పుడు మన ముఖ కవలికలు ఎలా ఉన్నాయో గుర్తించగలదు.
- ఫేస్ రికగ్నిషన్ సాఫ్ట్‌వేర్ ఉంటే, మన ముఖ కొలతల ఆధారంగా మన త్రీడీ మోడల్‌ను తయారుచేయడం కూడా అత్యంత సులభం.

యాప్‌లు మాత్రమే కాదు. స్పైవేర్‌లు, మాల్‌వేర్‌లు కూడా ఈ పని చేస్తాయి. ఫలానా చాక్లెట్ కంపెనీ వార్షికోత్సవం సందర్భంగా చాక్లెట్ బాక్సులు ఉచితంగా ఇంటికి పంపిస్తోంది. మీకు కూడా ఒకటి కావాలంటే ఈ లింక్‌ను క్లిక్ చేయండి లాంటి మెసేజ్‌లను చూసి ఆశపడ్డారో... ఇక మీ పని అంతే! ఆ లింకును క్లిక్ చేస్తే మీకు చాక్లెట్ బాక్స్ రాదు. కానీ, మీకు తెలియకుండానే స్పైవేర్ మీ ఫోన్‌లో చొరబడుతుంది. పాస్‌వర్డ్‌ల నుంచి వ్యక్తిగత సమాచారం వరకూ సమస్తం చోరీకి గురయ్యే ప్రమాదం ఉంది.

అలాంటి యాప్స్ జోలికెళ్ళొద్దు :

'మీరు ఏ హీరోలాగా ఉంటారు? ఏ హీరోయిన్ పోలికల్లో ఉంటారు? వచ్చే జన్మలో మీరు ఎలా పుడతారు?' లాంటి సరదా అప్లికేషన్లను క్లిక్ చేసేముందు జాగ్రత్త. అవి మీ సమాచారాన్ని సేకరిస్తాయి. అలాగే ఏదైనా యాప్‌ను ఇన్‌స్టాల్ చేసేటప్పుడు ఏ పర్మిషన్ అడిగితే ఆ పర్మిషన్ ఇవ్వొద్దు. ఉదాహరణకు ఏదో ట్రావెల్ బుకింగ్ యాప్ ఇన్‌స్టాల్ చేస్తున్నారనుకుందాం. దానికి కెమెరా పర్మిషన్ అవసరం లేదు. అయినా అడిగిందంటే అనుమానించాల్సిందే. ప్లేస్టోర్‌లో ఉన్న యాప్స్ అన్నీ సురక్షితమని చాలామంది అనుకుంటారు. కానీ కాదు. ప్లేస్టోర్లో బౌన్సర్ మెకానిజం ఉంటుంది. దాని ద్వారా అనుమానాస్పద యాప్స్‌ను దాదాపు 80% మేర వడపోస్తోంది. అన్నిటికన్నా ముఖ్యం... ఏదైనా యాప్ ఇన్‌స్టాల్ చేసే ముందు ఎండ్ యూజర్ లైసెన్స్ అగ్రిమెంటును చదవడం తప్పనిసరి. మరీ పదుల సంఖ్యలో పేజీలు ఉంటే కనీసం పైపైన అయినా ఒకసారి చూడడం మంచిది. లేకుంటే దెబ్బ తింటాం.

ఈ జాగ్రత్తలు తీసుకోండి :

ఇప్పుడు అన్ని మొబైల్ సంస్థలు అన్ లిమిటెడ్ డేటా సదుపాయాన్ని అందిస్తున్నాయి. కాబట్టి ఉచిత వైఫైల జోలికి వెళ్లకపోవడం మంచిది. ఆ నెట్‌వర్క్‌ను హ్యాకర్ యాక్సెస్ చేస్తే... వైఫైను వాడుతున్న అన్ని పరికరాల్లోకి ఏకకాలంలో మాల్‌వేర్, ట్రోజన్‌లను పంపగలడు.

- ఫోన్ సెక్యూరిటీ సెట్టింగ్స్‌లో 'అన్‌నోన్ సోర్సెస్' నుంచి డౌన్‌లోడ్ చేసిన యాప్స్‌ను ఇన్‌స్టాల్ చేసే సదుపాయాన్ని డిజేబుల్ చేయాలి.

- అవసరంలేని యాప్స్‌ను అస్సలు డౌన్‌లోడ్ చేసుకోవద్దు.
- చైనా ఫోన్ల విషయంలో జాగ్రత్తగా ఉండాలి. ఊరూపేరూ లేని ఫోన్లు చవకగా వస్తున్నాయని తీసుకుంటే.. అందులో మాల్‌వేర్ ప్రమాదం ఎక్కువగా ఉంటుంది. బ్రాండెడ్ ఫోన్లు ఎప్పటికప్పుడు ఆండ్రాయిడ్ సాఫ్ట్‌వేర్‌ను అప్‌డేట్ చేస్తాయి.
- వాట్సాప్, ఇతర మెసేజింగ్ యాప్‌లలో వచ్చే కొన్ని లింకులను క్లిక్ చేసినా... ట్రోజన్లు మీకు తెలియకుండా మీ ఫోన్‌లోకి దూరిపోతాయి. అవి హ్యాకర్లకు మీ ఫోన్‌ను యాక్సెస్ చేసే హక్కులు ఇస్తాయి.

24. విమానాశ్రయాలే అడ్డాగా ... సైబర్ మోసాలు

అమాయకులను నమ్మించి లక్షలు కాజేస్తున్న కేటుగాళ్ళు :

సైబర్ కేటుగాళ్ళు ఇటీవల విమానాశ్రయాలను కేరాఫ్ అడ్రస్‌గా వాడుకుంటున్నారు. అత్యాశకు పోయి వారి వలలో చిక్కిన బాధితులు లక్షల రూపాయలు పోగొట్టుకుంటున్నారు.

కస్టమ్స్ అధికారులు పట్టుకున్నారంటూ :

నగరానికి చెందిన ఓ యువతి షాదీ డాట్ కామ్‌లో వరుడి కోసం తన ప్రొఫైను అప్‌లోడ్ చేసింది. అమెరికాకు చెందిన ఓ వ్యక్తి నుంచి పెళ్లి ప్రపోజల్ వచ్చింది. అతడి ప్రొఫైల్ చూసిన యువతి అమెరికాలో డాక్టర్‌గా పనిచేస్తున్న వ్యక్తి తనను భాగస్వామిగా చేసుకోవడానికి ముందుకు వచ్చాడని సంబరపడింది. ఇద్దరూ ఒకరికొకరు ఫోన్ నంబర్లు ఇచ్చి పుచ్చుకున్నారు. వాట్సాప్, ఫేస్‌బుక్‌లో చాటింగ్ చేసుకున్నారు. ఇద్దరి అభిప్రాయాలు కలవడంతో పెళ్లికి సిద్ధమయ్యారు. ఫలానా తేదీన నేను ఇండియాకు వస్తున్నానని, వీలైతే అక్కడే భారతీయ సాంప్రదాయం ప్రకారం పెళ్లి చేసుకుందామని యువతిని నమ్మించాడు.

వచ్చేటప్పుడు అమెరికా నుంచి చాలా గిఫ్టులు, అమెరికన్ డాలర్లు తెస్తున్నానని ఊదరగొట్టాడు. ఇది జరిగిన రెండు రోజులకు ఫోన్ చేసిన కేటుగాడు 'నేను ఇండియా వచ్చాను. బెంగుళూరు ఎయిర్‌పోర్టులో దిగాను. కస్టమ్స్ అధికారులు పట్టుకున్నారు. గిఫ్టులు, డాలర్లకు కస్టమ్స్ సుంకం చెల్లించాలంటున్నారు. నా వద్ద డబ్బులు లేకపోవడంతో వస్తువులతో పాటూ రూ.50లక్షల విలువైన డాలర్లు సైతం సీజ్ చేశారు' అని చెప్పాడు. కస్టమ్స్ డ్యూటీ చెల్లించడానికి ఆ యువతి అతడు చెప్పిన అకౌంట్లో రూ.6 లక్షలు జమచేసింది. డబ్బులు అందగానే ఫోన్ స్విచ్ఛాఫ్ చేశాడు. ఆమె అతడికోసం ఆరా తీయగా... అదంతా మోసమని తేలడంతో పోలీసులను ఆశ్రయించింది.

అటవీ గింజలకు డిమాండ్ ఉందంటూ ...

నగరానికి చెందిన యువకునికి ఫేస్‌బుక్‌లో అమెరికాకు చెందిన ఓ ఇంగ్లీష్ మహిళ పరిచయం అయింది. తను ఓ ఫార్మా కంపెనీలో ఉన్నత హోదాలో పనిచేస్తున్నానని చెప్పింది. కొద్దిరోజుల తర్వాత ఓ బిజినెస్ డీల్ గురించి ఆ యువకుడికి చెప్పింది. కొద్దికాలంలోనే మీరు కోటీశ్వరులు కావొచ్చని అతడిని నమ్మించింది.

ఇండియాలో కొన్ని అటవీ ప్రాంతాల్లో మాత్రమే అరుదుగా దొరికే వాల్‌నట్స్ (ఒక రకమైన అటవీ గింజలు) పేరు చెప్పింది. వాటిని కేన్సర్ సంబంధిత ఔషధాల తయారీలో వాడతామని, వాటికి అమెరికాలో చాలా డిమాండ్ ఉందని నమ్మించింది.

ఆమె చెప్పినట్టుగా వాటిని అమ్మేవారిని ఫోన్‌లో సంప్రదించాడు. వారు చెప్పిన అకౌంటుకు రూ.5 లక్షలు పంపించగా ఆ గింజలను పార్సిల్‌లో పంపించారు.

ఈ విషయం ఆమెకు చెప్పాడు. మా కంపెనీ ఎగ్జిక్యూటివ్‌లు ఫలానా సమయంలో హైదరాబాద్ ఎయిర్‌పోర్టులో మిమ్మల్ని కలుస్తారు. మీరు కొనుగోలు చేసిన నట్స్‌ను వారికి చూపించండి అని చెప్పింది.

అవి నమ్మిన యువకుడు విమానాశ్రయంలో ఆమె చెప్పినట్టు కంపెనీ ఎగ్జిక్యూటివ్‌లను కలిశాడు. గింజలను చూసి ఇవే అని నిర్ధారించారు. ఎక్కువ మొత్తంలో పంపాలని సూచించి వెళ్లిపోయారు.

వెంటనే వారు ఆ యువకునికి మరో రూ. 10 లక్షలు చెల్లించి మరికొన్ని పంపాలని అమ్మకందారులను కోరాడు. వారం రోజులు గడిచినా గింజలను పంపించకపోవడంతో ఫేస్‌బుక్ ద్వారా మహిళకు చెబుదామని ప్రయత్నించగా ఖాతా క్లోజ్ చేసింది.

ఫోన్ చేయగా స్విచ్ఛాఫ్ వచ్చింది. గింజలను చూసి వెళ్లిన వారు ఫోన్ స్విచ్ఛాఫ్ చేశారు. మోసపోయానని గ్రహించిన ఆ యువకుడు పోలీసులను ఆశ్రయించాడు. ఇదంతా ఇండియాలో ఉంటూ నైజీరియా ముఠాలు చేస్తున్న సైబర్ మోసాలని పోలీసులు చెప్పారు.

విమానాశ్రయం పార్కింగ్‌లో కారు ఉందనీ.. అమ్ముతామంటూ OLXలో పెట్టి వనస్థలిపురానికి చెందిన రామిరెడ్డిని మోసం చేశారు.

ఇలా పలురకాల మోసాలకు పాల్పడుతున్న సైబర్ కేటుగాళ్ళు విమానాశ్రయాలను తమకు అనుకూలంగా మార్చుకుంటున్నారు. డబ్బున్న అమాయకులకు అత్యాశ చూపించి మోసం చేస్తున్నారు.

ఇలాంటి మోసాల పట్ల అప్రమత్తంగా ఉండాలని పోలీసులు సూచిస్తున్నారు.

సైబర్ నేరగాళ్ళతో జాగ్రత్తగా ఉండాలి ...

సైబర్ నేరగాళ్లు విమానాశ్రయాల పేర్లను సైతం వాడుకొని మోసాలకు పాల్పడుతున్నారు. ఎయిర్‌పోర్టులో కారు ఉందని, గిఫ్టులు, డాలర్లు కస్టమ్స్ అధికారులు పట్టుకున్నారు... వంటి కారణాలు చెప్పి అమాయకులను నమ్మించి దోచుకుంటున్నారు.

కేటుగాళ్ళు చెప్పేవి నిజమా... కాదా? అనేది తెలుసుకోవాలి.

కస్టమ్స్ అధికారులు పట్టుకున్నారని చెబితే... సెంట్రల్ ఎక్సైజ్ అండ్ కస్టమ్స్ వెబ్‌సైట్‌లోకి వెళ్ళే అధికారుల ఫోన్ నంబర్లు తెలుసుకుని వారికి ఫోన్ చేసి విషయం తెలుసుకోవాలి. ముక్కూ... మొఖం తెలియనివారు చెప్పే మాటలు నమ్మి లక్షల రూపాయలు పోగొట్టుకోవద్దు.

25. భీమా కంపెనీల పేరిట మోసాలు

మీరు భీమా ప్రీమియం చెల్లిస్తున్నారా? మీ పాలసీ బోనస్ ఇస్తామని ఫోన్లు వస్తున్నాయా? తక్కువ వడ్డీకే రుణం కావాలంటే మా కంపెనీలో ఒక పాలసీ చేయండి అంటూ సూచిస్తున్నారా? అయితే వీటికి మీరు స్పందించకండి. ఎందుకంటే ఇవన్నీ సైబర్ నేరస్తులు చేస్తున్నారని పోలీసులు చెబుతున్నారు.

ఈ కంపెనీలు మెట్రో నగరాల ప్రజలను లక్ష్యంగా చేసుకొని మోసం చేస్తున్నాయి. కొత్త పాలసీలు మధ్యలో వదిలేసినా పాలసీ వివరాలను ఐఆర్‌డీఏ పొరుగు సేవల సిబ్బంది నుంచి తీసుకుంటున్నారు. దీంతో పాటు పాలసీలు పునరుద్ధరిస్తాం.

కమీషన్ ఇవ్వాలంటూ ప్రైవేట్ భీమా కంపెనీలతో ఒప్పందాలు కుదుర్చుకొని తీసుకుంటున్నారు. అనంతరం ఎల్ఐసి సహా ప్రైవేట్ కార్పొరేట్ సంస్థల భీమా పాలసీదారులను లక్ష్యంగా చేసుకొని అక్రమాలకు పాల్పడుతున్నారు. ఏజెంట్ల ఒత్తిడి, ఆదాయపన్ను కారణంగా పాలసీతీసుకొని మధ్యలో వదిలేసిన వారి పేర్లు, చిరునామాలు తీసుకొని మీ పాలసీలకు బోనస్ డబ్బులిస్తున్నాం అంటూ మోసం చేసి వారి నుంచి లక్షల రూపాయిలు స్వాహా చేస్తున్నారు.

భీమా పాలసీదారులను మోసం చేసి లక్షల రూపాయలు స్వాహా చేసేందుకు సైబర్ నేరస్తులు కార్పొరేట్ తరహాల్లో కార్యాలయాలను ఏర్పాటు చేశారు. అనంతరం పదుల సంఖ్యల్లో టెలికాలర్లను నియమించుకున్నారు. వీరికి భీమా పాలసీదారులను ఎలా మోసం చేయాలి. ఏఏ ఖాతాల్లో నగదు జమచేయించాలన్న అంశాలను దొంగ భీమా కంపెనీల యజమానులు శిక్షణ ఇస్తున్నారు.

ఢిల్లీలోని కీర్తినగర్ జనక్‌పూరి, ఉత్తమ్‌నగర్, పశ్చిమ విహార నారాయణ్ ప్రాంతాల్లో 70కి పైగా ముఠాలు సుమారు వంద కార్యాలయాలను ఏర్పాటు చేశాయి. ఈ ముఠాల నాయకులు ఇంటర్మీడియేట్, డిగ్రీ వరకు మాత్రమే చదువుకున్నారు. వీరిలో ప్రైవేట్ భీమా కంపెనీల పాలసీలు చేయించి మధ్యలో మానేసిన వారున్నారు. భీమా పాలసీ కట్టి మధ్యలో వదిలేసినా వ్యక్తితో మాట్లాడి దశలవారీగా అతడు / ఆమెతో మాట్లాడి డబ్బులు కంపెనీ ఖాతాలో జమ చేయించాలి.

మోసపోయినవారి నుంచి రూ.లక్ష వరకు జమ చేయిస్తే వారికీ కమీషన్ ఇస్తున్నారు. ఇలా ఒక్కో కంపెనీ నిర్వహణ ఖర్చులన్నీ పోగా నెలకు రూ.15 లక్షల నుంచి రూ.25 లక్షలు ఆదాయం పొందుతున్నారు.

మధ్యలో వదిలేసిన పాలసీలకు రూ.లక్షల్లో డబ్బులిస్తామంటూ మోసగాళ్ళు ఆశపెడుతుండడంతో బాధితులు వారి వలలో చిక్కుతున్నారు. పేరు, పాలసీ వివరాలు, ఫోన్ నెంబర్లన్నీ సరిగా ఉండడంతో కంపెనీ అధికారులే మాట్లాడుతున్నారని అనుకుంటున్నారు. రూ.10లక్షల పాలసీకి రూ.40 లక్షల బోనస్ ఇస్తారంటూ చరవాణిలో చెప్పడం, దరఖాస్తుల ప్రాసెసింగ్ పేరుతో రూ. వేలు మాత్రమే అడగడంతో నేరగాళ్ల ఖాతాల్లో డబ్బు జమ చేస్తున్నారు.

నేరస్తులు బాధితులను నమ్మించేందుకు నకలు చెక్కులను కూడా పంపుతున్నారు. తాజాగా ఫిలింనగర్‌లో నివాసముంటున్న ఓ వ్యాపారి నుంచి మాక్స్ లైఫ్ ఇన్సూరెన్స్ పేరుతో ఫోన్‌చేశారు. ఒకసారి ప్రీమియం చెల్లిస్తే చాలు. మీకు ఐదేళ్ళలో రూ. 25 లక్షల నగదు వస్తుందని వివరించారు. ఆయన ఇదెలా సాధ్యమౌతుందని ప్రశ్నించగా... తమ కంపెనీ కొత్త విధానాలను అవలంభిస్తోందని వివరించారు. వారి మాటలు నమ్మిన వ్యాపారి రూ. 5 లక్షలు ఆన్‌లైన్ ద్వారా బదిలీ చేశారు. తర్వాత మాక్స్ లైఫ్ ప్రతినిధులంటూ చెప్పుకొన్నవారికీ ఫోన్ చేయగా స్పందించలేదు. దీంతో మోసపోయానని గ్రహించిన ఆయన సైబర్ క్రైమ్ పోలీసులకు ఫిర్యాదు చేశారు. కావున మీవి ఏమైనా ఇలాంటి భీమా పాలసీ సమస్యలు ఉంటే నేరుగా స్థానిక కార్యాలయంలో సంప్రదించి ఈ సమస్యను తీర్చుకోవాలే గాని ఫోన్ ద్వార సంప్రదించిన కొత్త వ్యక్తులను ఎట్టి పరిస్థితులలో నమ్మవద్దు. వారు చెప్పిన అకౌంటులలో డబ్బు వేయవద్దు.

26. ఓఎల్ఎక్స్ లక్ష్యంగా మోసాలు

సెకండ్ హ్యాండ్ (పాతవి) వస్తువులు ఏవైనా అమ్మాలన్నా... కొనాలన్నా అందరూ ఇప్పుడు OLXలోనే వెతుకుతున్నారు. ఇంట్లో నుంచి బయటకు వెళ్లకుండానే మనకు కావలసిన వస్తువులు... కావలసిన బడ్జెట్‌లో కొనుక్కునే / అమ్ముకునే సౌలభ్యం వుంటుందనే భావనతో అందరూ దీనిపైనే ఆధారపడుతున్నారు. ప్రధానంగా యువతను మరింతగా ఆకట్టుకోవడంతో దీనికి ఆదరణ పెరిగింది. మోసాలకు అలవాటు పడిన వాళ్లు ఇప్పుడు దీనిపై కన్నేశారు.

OLXలో అమ్మకానికి పెట్టే వస్తువులను కొంటామంటూ అవతలివారికి ఫోన్‌చేసి తమ నైపుణ్యంతో మభ్యపెట్టి వస్తువులను ఎత్తుకెళ్లిపోతున్నారు. అమ్మకందారులు ఆశించిన ధర కంటే ఎక్కువ ధర ఇస్తామంటూ ఆశపెట్టి తమ ఉచ్చులోకి లాగుతున్నారు. తీరా డబ్బులు ఇవ్వకుండానే వస్తువుని పట్టుకుని ఉడాయించేస్తున్నారు.

ఒక ఇంజనీరింగ్ విద్యార్థి తాను వాడుతున్న ఐఫోన్ 7ఎస్‌ని అమ్మకానికి OLXలో పెట్టాడు. ధర రూ. 45వేలుగా పేర్కొని ఆసక్తి వున్నవాళ్లు సంప్రదించేందుకు తన ఫోన్ నంబరును కూడా పెట్టాడు. శనివారం ఉదయం గుర్తు తెలియని వ్యక్తి నుంచి ఇంజనీరింగ్ విద్యార్థికి ఫోన్ వచ్చింది. OLXలో పెట్టిన ఫోన్‌ను తాను కొనాలనుకుంటున్నానని, ఫోన్‌ను ఒకసారి చూస్తే బేరం మాట్లాడుకుందామని చెప్పాడు. ఒకరోజు ఎస్‌బీఐ వద్ద ఇద్దరూ కలిశారు. సెల్‌ఫోన్ చూసి రూ. 40 వేలు అయితే కొనాలనుకుంటున్నానని అవతలి వ్యక్తి చెప్పడంతో ఇంజనీరింగ్ విద్యార్థి సరేనన్నాడు. బ్యాంకు అకౌంట్ నంబరు చెబితే డబ్బులు ఆన్‌లైన్ ట్రాన్స్‌ఫర్ చేసేస్తానని చెప్పడంతో తన బ్యాంక్ అకౌంట్ నంబరు చెప్పాడు. ట్రాన్స్‌ఫర్ అయిపోయిందని ఒకసారి ఏటీఎం వద్దకు వెళ్ళి చెక్ చేసుకోవాలని అవతలి వ్యక్తి చెప్పాడు. సెల్‌ఫోన్‌ని అవతలి వ్యక్తి చూస్తుండటంతో మొహమాటం కొద్దీ సెల్‌ఫోన్‌ను అడగకుండా నేరుగా ఏటీఎం లోకి వెళ్లి బ్యాలెన్స్ చెక్ చేశాడు. డబ్బులు ట్రాన్స్‌ఫర్ కాకపోవడంతో ఆ విషయం చెప్పేందుకు బయటకు వచ్చాడు.

అక్కడ వుండాల్సిన వ్యక్తి కూడా కనిపించకపోవడంతో తనకు వచ్చిన కాల్ ఆధారంగా ఆ నంబర్‌కు ఫోన్ చేశాడు. ఫోన్ స్విచ్ఛాఫ్ అని రావడంతో తాను మోసపోయినట్టు నిర్ధారించుకున్నాడు. ఆదివారం ఉదయం పోలీసు స్టేషన్‌కు వెళ్లి దీనిపై ఫిర్యాదుచేశాడు.

ఆశించిన ధర కంటే అధికంగా ఇస్తామంటూ ఉచ్చులోకి ...

ఏదైనా వస్తువు అమ్మకానికి పెట్టిన వ్యక్తులకు ఫోన్ చేసి ధరపై ఫోన్ లోనే బేరం ఆడుతున్నారు. అమ్మకందారుడు ఆశించిన ధర కంటే ఎక్కువ ధర ఇచ్చేందుకు సుముఖంగా ఉన్నట్లు నటించి వారిని తమ ఉచ్చులోకి లాగుతున్నారు.

తాను ఆశించిన ధర కంటే ఎక్కువ ధర వస్తుందని అమ్మకానికి పెట్టిన వ్యక్తి సంబరపడి ఎలాగైనా అతనికి అమ్మేయాలనే భావన ఏర్పరచుకుంటున్నాడు. ఒకవేళ తాను జాప్యం చేస్తే అవతలి వ్యక్తి కొనుగోలు చేయకుండా వెనకడుగు వేసేస్తాడేమోననే భయంతో అవతలి వాళ్లు ఎక్కడికి రమ్మంటే అక్కడికి వస్తువుతో సహా వెళ్లిపోతున్నారు.

ఒకవేళ ఏ విషయంలోనైనా మొండిగా వ్యవహరిస్తే డీల్ చెడిపోతుందనే భయంతో ఒకింత మొహమాటంగా వ్యవహరించాల్సిన పరిస్థితి ఏర్పడుతోంది. దీనికోసమే ఎదురుచూస్తున్న మోసగాళ్లు తమ చేతివాటాన్ని ప్రదర్శించి వస్తువుతో సహా ఉడాయించేస్తున్నారు. చివరకు తాను ఫోన్ చేసిన నంబర్ చిక్కకుండా వుండేందుకు సిమ్‌కార్డు తీసి పారేస్తున్నారు.

అదేవిధంగా దొంగిలించిన వాహనాలు మరియు వస్తువులను ఇటీవల OLX ద్వారా అమ్మడం అనేది జోరు అందుకుంది. కాబట్టి కొనుగోలుదారులు చాలా జాగ్రత్త వహించాలి.

ఇంకొక రకం మోసం ఏమిటంటే ఒక విలువైన కారు OLXలో తక్కువ ధరకే అమ్మకానికి ఉంచిన వ్యక్తి ఫోన్ ద్వారా సంప్రదించిన వ్యక్తులను వారు ఆ వాహనాన్ని ఫలానా ఎయిర్‌పోర్టులో పార్కింగ్ ప్లేస్‌లో ఉంచాము. మీరు ప్రత్యక్షంగా చూసుకొని బేరం చేయవచ్చు అని నమ్మించి ఉత్తర భారతదేశ దొంగలు కొందరు నమ్మకంగా అక్కడికి పిలిపించుకొని వారిని నమ్మించి మారు మూలల పల్లెలకు తీసుకెళ్ళి అక్కడ వారిపై దాడిచేసి కొట్టి నగదు లాక్కొని వారి ఏటీఎం కార్డులు తీసుకొని దాని పిన్ నెంబర్ కనుక్కొని అందులోని సొమ్ము దోచుకొని ఆ పిమ్మట ఫోన్ ద్వారా వారి కుటుంబసభ్యులతో మాట్లాడించి మీ వారిని కిడ్నాప్ చేశామని వారిని విడిపించుకోవాలంటే 5 లేక 10 లక్షలు తాము చెప్పే ఎకౌంటులో వేయాలని చెప్పి బెదిరించి, బేరమాడి ఆ సొమ్ము కూడా అకౌంటులోని తెప్పించుకొని దారి ఖర్చులకు డబ్బు ఇచ్చి వారిని వదిలిపెడుతున్న సంఘటనలు కొన్ని జరిగాయి. కావున OLXలో వాహన కొనుగోలు విషయం అంటే గుడ్డిగా నమ్మి మోసపోవద్దు.

అప్రమత్తత తప్పనిసరి ...

యువత ఎక్కువగా OLXను వాడుతుండడంతో మోసాలకు గురయ్యే అవకాశం ఉంది. వస్తువు నాణ్యత, ధరను పరిశీలించుకోవాలి. కొనుగోలు / అమ్మకం చేయాలా? వద్దా? అనే దానితో పాటూ ఆ వస్తువు అంత విలువ చేస్తుందా? లేదా? అని చూసుకోవాల్సిన బాధ్యత లావాదేవీలు జరిపేవాళ్ళదే. డబ్బులు చేతికి అందిన తర్వాతే వస్తువును వారికి ఇవ్వాలి. ఒకవేళ అకౌంట్‌కి వేస్తే పడినట్లు నిర్ధారించుకున్న తర్వాతే వస్తువు అందజేయాలి. మొహమాటానికి పోతే మొదటికే మోసం ఎదురయ్యే ప్రమాదం వుందని గ్రహించాలి.

సెల్‌ఫోనులోని వ్యక్తిగత రహస్య వీడియోలను సంగ్రహించి బ్లాక్ మెయిల్ :

ఇప్పటికే ఫోన్ హ్యాకింగ్ ద్వారా వ్యక్తిగత లావాదేవీలు, బ్యాంకు వివరాలు అపహరణకు గురై ఇబ్బందులు ఎదుర్కొంటున్న బాధితుల సంఖ్య వేల సంఖ్యలో ఉంది. తాజాగా అందులో దాచి ఉంచిన వ్యక్తిగత ఫోటోలు, వీడియోలు కూడా తస్కరిస్తున్నారు. వాటిని వివిధ సైట్లలో పోస్ట్ చేసి అక్రమార్జనకు పాల్పడుతున్నారు. చేతులు కాలాక ఆకులు పట్టుకున్న చందాన అసలు విషయం తెలుసుకునే సరికి జరగాల్సిన నష్టం జరిగిపోతుంది. దీంతో కొందరు పోలీసులను ఆశ్రయిస్తుండగా కొంతమంది పరువుపోతుందనే భయంతో మిన్నకుంటున్నారు.

స్మార్ట్ ఫోన్ వినియోగించడంలో చాలా మెళకువలు పాటించాల్సిందే. ఏ మాత్రం నిర్లక్ష్యం వహించినా భారీ మూల్యం చెల్లించాల్సి రావచ్చు. మన ఫోన్ కదా అని ఇష్టానుసారంగా ఫోటోలు, వీడియోలు రికార్డు చేసి భద్రపరచడం ప్రమాదకరం. ముఖ్యంగా యువతీయువకులు సరదాకోసం తీసుకునే ఫోటోలు, వీడియోలు ఫోన్‌లోనే సేవ్ చేసి ఉంచుతారు.

కొన్ని సందర్భాల్లో భార్యాభర్తల మధ్య సంభాషణలు, వారి వ్యక్తిగత ఫోటోలు, వీడియోలు కూడా రికార్డు చేసుకోవడం ఓ ఫ్యాషన్‌గా మారింది. ఫోన్‌లో సేవ్ చేసిన తర్వాత జాగ్రత్తగా రక్షించుకోవాలి. సేవ్ చేసే సమయంలో జాగ్రత్త పడాలి. ఒకవేళ మీ చేతి వేళ్ళ ద్వారా అనుకోనివిధంగా బటన్‌లు నొక్కితే సోషల్ మీడియా లేదా ఇతర మాధ్యమాల ద్వారా ఇతరుల చేతుల్లోకి అవి వెళ్ళే ప్రమాదముంది.

కొన్ని సందర్భాల్లో ఫోన్ పోగొట్టుకున్నా మీ వ్యక్తిగత వివరాలు ఇతరుల చేతుల్లోకి వెళ్లినట్టే. అదెక్కడో బూతు సైట్లోనో లేక ఇతర ప్రమాదకర వెబ్‌సైట్లలోనో దర్శనమిచ్చే ప్రమాదముంది. ఆ తర్వాత ఇబ్బందులు ఎదుర్కొనేకన్నా.. ముందుజాగ్రత్తలే మేలు.

మీ ఫోనులో ఏదైనా సమస్య వచ్చినప్పుడు దాన్ని సర్వీస్ సెంటర్‌లో ఇచ్చినపుడు అక్కడి వారు మీ ఫోన్‌ను క్షుణ్ణంగా పరిశీలించినప్పుడు మీ వ్యక్తిగత రహస్య ఫోటోలు, వీడియోలు బయటపడతాయి. వాటిని మీకు తెలియకుండా చోరీ చేసి ఆ తరువాత మిమ్మలను బ్లాక్ మెయిల్ చేసి డబ్బు డిమాండ్ చేయవచ్చు లేదా అవి బూతు వెబ్‌సైట్‌లో దర్శనమివ్వచ్చు.

స్మార్ట్‌ఫోన్‌లో దాచొద్దు

స్మార్ట్ ఫోన్ల వినియోగంలో మెయిల్ ఐడీ కూడా అనుసంధానం చేయాల్సి నిబంధన ఉంటుందనే విషయాన్ని గుర్తించి ఎప్పటికప్పుడు ఇంటర్నెట్‌తో అనుసంధానం చేస్తున్న సమయాల్లో కూడా తగిన జాగ్రత్తలు తీసుకోవాలి.

అసలు వ్యక్తిగత వీడియోలు, ఫోటోలు తీసేసిన తర్వాతనే అనుసంధాన ప్రక్రియ సాగిస్తుండాలి. అన్నింటికన్నా ఉత్తమం అలాంటి ఫోటోలు, వీడియోలు తీయకుంటే చాలా మంచిది.

ప్రేమ వ్యవహారాల్లో కూడా ఇలాంటి సమస్యలు పెరుగుతున్నాయి. సన్నిహితంగా ఉంటున్న సమయంలో మాటలతో నమ్మించి ఫోటోలు, వీడియోలు తీస్తున్నారు. ఏమాత్రం తేడా వచ్చినా వాటిని పోస్ట్ చేసి యువతుల జీవితాలతో చెలగాటమాడుతున్న పోకిరీల సంఖ్య కూడా ఇటీవల పెరుగుతూ వస్తోంది.

భార్యాభర్తలు కలిసివున్న ఫోటోలు, వీడియోలు తీసిన తర్వాత భార్యలనే బ్లాక్ మెయిల్ చేసిన ప్రబుద్ధుల గురించి కూడా ఫిర్యాదులు అందాయంటే ఈ పైశాచికత్వం ఏ దశలో ఉందో గమనించవచ్చు.

పెరుగుతున్న కేసులు :

వ్యక్తిగత ఫోటోలు, వీడియోల ద్వారా పెరిగిపోతున్న వేధింపులు ... సోషల్ మీడియాలో అప్‌లోడ్ చేస్తామని బ్లాక్ మెయిలింగ్‌లకు పాల్పడుతున్న సంఘటనలు వేలసంఖ్యలో వెలుగు చూస్తున్నాయి. ఫిర్యాదు వచ్చిన తర్వాత ధర్యాప్తు చేపట్టి నిందితులను అరెస్టు చేస్తున్నప్పటికీ చాలామంది ఫిర్యాదు చేయడానికి ముందుకు రావడం లేదనే వాదనలు కూడా వినిపిస్తున్నాయి. సన్నిహితంగా ఉన్నపుడు తీసిన ఫోటోలు, వీడియోలు వారి జీవితంలోనే మరపురాని మచ్చలుగా మిగిలిపోతున్నాయి. వారి ఫ్రెండ్‌షిప్‌లో తేడాలు వచ్చినప్పుడు... లేదా పెళ్ళికి అనుమతులు లభించినప్పుడు ఇలాంటి కేటుగాళ్ళు చీప్ ట్రిక్స్‌కు పాల్పడి ఫోన్ల ద్వారా తీసిన ఫోటోలు, వీడియోలను బజారుకీడుస్తున్నారు.

27. ఆన్‌లైన్ షాపింగ్... పొంచి ఉన్న మోసాలు

ఆన్‌లైన్‌లో షాపింగ్ చేయడం సరదాగా మారింది. ఇంటర్నెట్ గురించి అంతగా అవగాహన లేనివారు ఇంట్లో టీవీ చానెళ్ళు కూడా షాపింగ్ చేసేస్తున్నారు. అంతా సజావుగా సాగితే ఇబ్బంది లేదు. ఆన్‌లైన్‌లో షాపింగ్ చేసే సమయంలో ఇచ్చే వివరాలు బయటకు పొక్కడంతో కస్టమర్లకు కొత్త చిక్కులు తెచ్చిపెడుతున్నాయి. ఆర్డర్ పూర్తయిన తర్వాత కొంతమంది స్వార్థం వల్ల ఆ డేటా క్రిమినల్స్ చేతుల్లోకి వెళుతోంది. దీంతో ఆన్‌లైన్ కస్టమర్లు మోసాల బారిన పడే ప్రమాదాలు ముంచుకొస్తున్నాయి. వినియోగదారులు ఉత్సాహంగా షాపింగ్ చేయడం, వస్తువులను నేరుగా ఇంటికి రప్పించుకోవడంపై ఆసక్తి కనబరుస్తున్నారు. దానికోసం ఆయా వైబ్‌సైట్లు సూచించిన విధంగా వ్యక్తిగత వివరాలు, ఆన్‌లైన్ పేమెంట్ లేదా డెబిట్ / క్రెడిట్ కార్డు ద్వారా డబ్బులు చెల్లించేస్తున్నారు. ఇన్ని వివరాలు చెప్పిన తర్వాత కస్టమర్లకు భద్రత ఉందా? అంటే అన్నీ అనుమానాలే. ఆన్‌లైన్ ద్వారా చెల్లింపులు చేస్తే ఇబ్బందులు తలెత్తవని మరికొందరి వాదన. జాగ్రత్తగా చేస్తే సమస్య ఉండదు. ఏమరుపాటుగా ఉంటే చిక్కుల్లో పడక తప్పదని జరుగుతున్న ఘటనలే నిదర్శనం. వ్యక్తిగత వివరాలను బహిర్గతం చేయరాదంటూ కొన్నాళ్లుగా వివిధ మాధ్యమాల ద్వారా ప్రచారం జరుగుతూనే ఉంది.

సమస్యలు :

➲ ఆన్‌లైన్ షాపింగ్ ద్వారా వ్యక్తిగత సమాచారం బయటకు వెళుతోంది. దాని ఆధారంగా మీ పేరిట బ్యాంక్ అకౌంట్లు తెరవడం, ఆన్‌లైన్‌లో కొనుగోలు చేయడం, క్రెడిట్ కార్డులు తీసుకోవడం సాధ్యమవుతుందని సాఫ్ట్‌వేర్ నిపుణులు చెబుతున్నారు. ఆయా వివరాలను కీబోర్డు ద్వారా పొందుపరచే సమయంలో ట్రోజన్ హార్స్ అనే వైరస్ మీరు రాసే పదాలన్నీ (యూజర్ నేమ్, పాస్వర్డ్‌తో సహా) రికార్డు చేసి మోసగాళ్ళకు సహకరిస్తోంది.

- ఫిషింగ్... ఇది మీ ప్రమేయం లేకుండా డేటా సేకరించి క్రిమినల్స్ చేతిలో పెడుతుంది. ఇలాంటి మోసాలలో మీకు వచ్చే మెయిళ్ల ద్వారా ఆన్‌లైన్ స్టోర్స్ నుంచి వచ్చే మెయిల్స్‌ను క్లిక్ చేస్తూ మీ డేటాను సేకరిస్తారు.
- స్పామ్ మెయిల్ ద్వారా ఆన్‌లైన్ షాపర్స్ బేరమాడే వసతి కల్పించినట్లు తక్కువ ధరలో విలువైన వస్తువులు దొరుకుతున్నాయని భారీ వస్తువులు ఫ్రీగా వస్తున్నాయని మభ్యపెడతారు. దానికోసం కొంతమందిని ఆ మెయిల్ లేదా వాట్సాప్ మెసేజ్‌ను ఫార్వార్డ్ చేయమని చెప్పడంతో పాటూ విలువైన సమాచారాన్ని రాయమంటారు. ఆ వస్తువు ఫ్రీగా పొందాలంటే తక్కువ ధరకు వస్తున్న మరొకటి తప్పనిసరిగా కొనాలంటూ బ్యాంకు వివరాలు రాబడతారు.
- ఓవర్ పేమెంట్ పేరిట మోసాలు విపరీతంగా పెరుగుతున్నాయి. వస్తువు కొనుగోలు చేసినపుడు చెల్లించిన తర్వాత ఆ డబ్బులు చేరలేదని మోసగాళ్ళ నుంచి ఫోన్ వస్తుంది. ఒకవేళ డబ్బులు రెండుసార్లు చెల్లింపు జరిగితే ఓవర్ పేమెంట్‌ను తిరిగి ఇచ్చేస్తామని నమ్మిస్తారు. తొందరపాటుతో కొంతమంది డబ్బు రెండోసారి చెల్లించి మోసపోతున్నారు.
- నకిలీ ఆర్డర్ సృష్టించి కస్టమర్లను తప్పుదోవ పట్టిస్తుంటారు. ఒకరికి వెళ్లాల్సిన వస్తువు మీ చిరునామాకు చేరిందని, దాని విలువ కన్నా సగం రేటుకే ఉన్నట్లు ఆర్డర్ కాపీని సృష్టిస్తారు. మీకు అవసరం లేదంటే పర్వాలేదు.. కానీ మీరు దాన్ని కొనుగోలు చేస్తే వారికి వేరే ఆర్డర్ పంపిస్తామని చెప్తాడు. తక్కువ ధరలో వస్తున్నందుకు తొందరపడే వారే మోసగాళ్ళ లక్ష్యం.
- ఒక వస్తువు కొనుగోలు చేసిన తర్వాత మీ వివరాలు సేకరించే కేటుగాళ్ళు తిరిగి కాల్ చేసి బహుమతి వచ్చిందంటూ మభ్యపెడతారు. లక్షల విలువ చేసే కారు, ఇతర వస్తువుల ఆశ చూపించి దానికోసం ట్యాక్స్‌ల కింద కొంత చెల్లించాలని అందినంత దండుకుంటారు.

ఎలాంటి జాగ్రత్తలు తీసుకోవాలి..

- ఆర్డర్ ఇచ్చే సమయంలో మంచి కంపెనీలు, నమ్మకమున్న సంస్థల ద్వారానే కొనుగోలు చేయాలి.
- కస్టమర్ సర్వీస్, కుటుంబీకులు, సన్నిహితుల సలహా తీసుకొని ఆన్‌లైన్ షాపింగ్ చేయాలి.
- వెబ్‌సైట్‌ను సందర్శించినపుడు కింద కస్టమర్ రివ్యూలు ఉంటాయి. వాటిని చదివితే ఆ సైట్ పై కొంత అవగాహన కలుగుతుంది.
- అధిక వివరాలు అడిగితే అనుమానించాలి.
- మెయిల్ ద్వారా వివరాలు అడిగినప్పుడు వారు పంపిన లింకును తెరవకుండా వెంటనే వెబ్‌సైట్ చెక్ చేసుకోవాలి. అవసరమైతే కస్టమర్‌కేర్ నంబరుకు ఫోన్ చేసి సందేహాలపై ఆరాతీయాలి.
- పబ్లిక్ స్థలాలు, ఇంటర్నెట్ కేంద్రాల నుంచి కంప్యూటర్ల ద్వారా వివరాలు షేర్ చేయకపోవడం మంచిది. వ్యక్తిగత కంప్యూటర్లు, ల్యాప్‌టాప్‌లలో సైతం యాంటీ మాల్‌వేర్, యాంటీ ఫిషింగ్, యాంటీ వైరస్ లాంటి సాఫ్ట్‌వేర్‌లను వాడాలి.

➡ వివరాలు పొందేటపుడు పేరు, అడ్రసు, బ్యాంక్ అకౌంట్ నంబర్, ఏటీఎం కార్డు నంబరు, పిన్ నంబరు, ఇతర వివరాలు మరలా మరలా నమోదు చేయనవసరం లేకుండా ఉండేందుకు సదరు వివరములు "సేవ్" చేయమంటారా అని కొన్ని సైట్లు అడుగుతుంటాయి. ఎలాంటి పరిస్థితులలో మీ వివరాలు ముఖ్యంగా బ్యాంకు ఏటీఎం, పిన్ నంబరు, సివివి నంబరు "సేవ్" చేయవద్దు. అవి మోసగాళ్ళ చేతిలో పడితే చాలా ప్రమాదము.

మీకు సంబంధించిన వ్యక్తిగత సమాచారాన్ని ఎట్టి పరిస్థితుల్లోనూ ఎవరితో షేర్ చేసుకోవద్దు. మీ వ్యక్తిగత పత్రాలను వెబ్‌సైట్లలో అప్‌లోడ్ చేయడమంటే మీ జుట్టును శత్రువుల చేతికి చిక్కేలా చేసుకున్నట్లే. ఫోన్లలో, మెయిళ్ళలో కూడా వాటిని ఎవరితో షేర్ చేసుకోవద్దు.

మీ నకళ్ళను చించేయండి...

ఏదయినా కార్యాలయంలో మీ అవసరం తీరిన తరువాత మీ దగ్గర ఇంకా ఏమైనా పత్రాల నకళ్ళుంటే వాటిని ఇంటికి తీసుకెళ్ళండి.

అంతేకానీ వాటిని అక్కడే పడేయటమో... చెత్తబుట్టలో వేయడమో చేయవద్దు. క్రిమినల్స్ వాటికోసమే వేచి ఉంటారు.

కొంతమందిని పనిగట్టుకుని పురమాయించి సదరు పత్రాలను వారు సంపాదించుకోవచ్చు. గుర్తింపు దొంగతనం అత్యంత సులువుగా జరిగే మార్గాల్లో ఇది ఒకటి.

ఏదైనా సిమ్‌కార్డు కొరకు గానీ, బ్యాంకు ఖాతా తెరవడం గానీ ఇతర అవసరాలకు మీ ధృవపత్రాలు ఇవ్వవలసి వస్తే ఒక్క కాపీ మాత్రమే ఇచ్చి అందులో ఖాళీ ప్రాంతంలో పెద్ద అక్షరాలతో ఈ పత్రం ఎప్పుడు, ఎందుకొరకు, ఎవ్వరికి యివ్వబడిందో స్పష్టంగా వ్రాయండి.

ఇందుకు విరుద్ధంగా ఉపయోగించినయెడల తగు చర్య తీసుకోబడుతుందని కూడా వ్రాయండి. అనవసరంగా మిగిలిపోయాయని జిరాక్స్ కాపీలను విరివిగా పంచకండి. లేకపోతే మీరు గుర్తింపు దొంగతనానికి గురికావచ్చు.

పాస్‌వర్డ్‌లు కాపాడుకోండి...

మీరు నమ్మండి, నమ్మకపోండి ... మీ పాస్‌వర్డులను ఏదైనా పుస్తకంలో రాసి ఉంచుకోవడం అత్యంత ఉత్తమ మార్గం. ఈ సలహా విని మీరూ నవ్వుకోవచ్చు.

ఈ డిజిటల్ యుగంలో కంప్యూటర్లలో మన సమాచారాన్ని స్టోర్ చేసుకునే అవకాశం ఉండగా, పాత చింతకాయ పచ్చడి ఐడియాలేంటని మీరు అనుకుంటే అనుకోవచ్చు. అమెరికాలో చాలామంది ఈ మధ్యకాలంలో ఈ విధానాన్ని ఫాలో అవుతున్నారు.

కంప్యూటర్ హార్డ్‌డ్రైవ్లలో ఇన్ఫర్మేషనును పెట్టుకునే లెక్కయితే దాన్ని ఎన్క్రిప్ట్ చేసి పెట్టుకోవడం మేలు. ఏ వెబ్‌సైట్ పడితే ఆ వెబ్‌సైటును క్లిక్ చేసి అందులో మీ వివరాలను నింపేయకండి. పాస్‌వర్డ్‌లను ఎప్పటికప్పుడు మార్చుకోండి.

28. ఈ ఫైలింగ్ & ఇన్‌కమ్ ట్యాక్స్ రీఫండ్ అప్రూవ్డ్ అంటూ సంక్షిప్త సందేశాలతో మోసం

ఐటీ రిటర్న్ ఫైల్ చేసిన తరువాత అధికంగా కట్ అయిన పన్ను రీఫండ్‌గా వస్తుంది. దీనికోసం ప్రతి పన్ను చెల్లింపుదారుడు తన బ్యాంకు ఖాతా వివరాలను రిటర్న్‌తో పాటే ఐటీ విభాగానికి తెలియజేస్తాడు. ఆ మొత్తం రీఫండ్ వచ్చే ముందు ఐటీ డిపార్ట్‌మెంట్ నుంచి ఓ సంక్షిప్త సందేశం వస్తుంది. దీన్నే సైబర్ నేరగాళ్ళు ఫిషింగ్ కోసం వినియోగించుకుంటున్నారు.

ఉత్తరాదిన తిష్టవేసిన ఈ నేరగాళ్ళు వివిధ మార్గాల్లో ఆదాయపు పన్ను చెల్లింపుదారుల సెల్ ఫోన్ నంబర్లకు ఐటీ విభాగం పంపినట్లు 'రీ ఫండ్ అప్రూవ్డ్' అంటూ ఎస్.ఎం.ఎస్.లు పంపుతున్నారు.

ఇందులో ఉద్దేశపూర్వకంగానే బ్యాంకు ఖాతా వివరాలు తప్పుగా పొందుపరుస్తున్నారు. దీంతో ఎస్.ఎం.ఎస్.లు చూసుకున్నవారు అందులో తమ బ్యాంకు ఖాతా వివరాలు తప్పుగా ఉన్నాయని, ఐటీ విభాగం ఇచ్చే రీఫండ్ అందులోకి వెళ్ళిపోతుందని భావిస్తున్నారు.

వెంటనే తమ ఖాతా వివరాలు అప్‌డేట్ చేయడానికి ఎస్.ఎం.ఎస్.లో నేరగాళ్ళు ఇచ్చిన లింకును క్లిక్ చేస్తున్నారు.

వరుసపెట్టి వివరాలు సేకరణ :

ఎస్.ఎం.ఎస్‌లోని లింకును క్లిక్ చేయడంతోనే వినియోగదారుడు "ఫిషింగ్" వెబ్ పేజ్‌లోకి ఎంటర్ అవుతున్నాడు. ఇందుకోసం సైబర్ నేరగాళ్ళు ఆదాయపు పన్ను శాఖ వెబ్‌సైట్‌ను పోలిందే మరోటి సృష్టించారు.

- అసలైన ఇన్‌కమ్ ట్యాక్స్ విభాగం వెబ్‌సైట్ అడ్రస్ బార్‌లో https://www.incometax indiafiling.gov.in/home అని ఉంటుంది. బోగస్ వెబ్‌సైట్ అడ్రస్ బార్ పరిశీలిస్తే http://50.63.185.184/~shndkfnlemdinsl/500599524/hqu.Php?Refund status=APPROVED&id=YWJjQDEyMy5jb20%3D గా ఉన్నట్లు గుర్తించవచ్చు.
- దీన్ని గమనించకుండా ఎవరైనా ముందుకెళ్తే బ్యాంకు ఖాతా వివరాలు పొందుపరచాలంటూ ప్రత్యక్షం అవుతుంది.
- ఈ లింకులో బ్యాంకును ఎంపిక చేసుకోండంటూ యాక్సిస్, సిటీ, హెచ్.డి.ఎఫ్.సీ, ఐసీఐసీఐ, ఎస్.బీ.ఐ పేర్లతో పాటూ "అదర్స్" ఆప్షన్ కనిపిస్తుంది.
- ఆయా బ్యాంకుల్లో ఖాతాలు ఉన్నవారు ఎవరైనా దాని పేరు ఎంచుకుని 'ప్రొసీడ్' నొక్కితే ఈ బ్యాంకు వెబ్‌సైట్‌ను పోలిందే నకిలీది ఓపెన్ అవుతోంది.

- ఉదాహరణకు ఎస్.బీ.ఐదే తీసుకుంటే అసలైన ఎస్.బీ.ఐ ఆన్‌లైన్ బ్యాంకింగ్ అధికారిక సైట్‌లోకి ఎంటర్ అయితే అడ్రస్ బార్‌లో https://retail.onlinesbi.com/retail/login.htm అని వస్తుంది. నకిలీ దాంట్లో ప్రవేశిస్తే అడ్రస్ బార్‌లో http://50.63.185.184/~shndkfnlemdinsl/500599524/hqu.Php?Refundstatus=APPROVED&id=YWJjQDEyMy5jb20%3D అని కనిపిస్తుంటుంది.
- దీన్ని కూడా గమనించకుండా వినియోగదారుడు ముందుకు వెళ్తే బ్యాంకు అధికారిక సైట్‌ను పోలి, అందులోని వివరాలతో కూడి ఉండే ఈ నకిలీ సైట్ యూజర్ నేమ్, పాస్‌వర్డ్‌తో పాటూ అన్ని వివరాలు పొందుపరచమని కోరుతుంది.

  తర్వాత వన్‌టైమ్ పాస్‌వర్డ్ అడుగుతుంది. సెల్‌ఫోన్ / మెయిల్ వచ్చిన పాస్‌వర్డ్‌ను పొందుపరచిన వెంటనే పూర్తి వివరాలు సైబర్ నేరగాళ్ళకు చేరిపోతాయి. అలా బ్యాంకు ఖాతాల్లోని నగదును లూటీ చేస్తారు.
- నకిలీ వెబ్‌సైట్స్‌లో ప్రవేశించినప్పుడు హెచ్చరిక కనిపిస్తుంది. సాధారణంగా అడ్రస్ బార్‌కు ఎడమవైపు https:// అనే అక్షరాలు ఉండే పక్కనే 'సెక్యూర్' అని కనిపిస్తుంది. ఈ వెబ్‌సైట్ సురక్షితం కాదని అర్థం.
- బోగస్ వెబ్‌సైట్ ఓపెన్ చేసినప్పుడు అడ్రస్ బార్ పక్కన (ఎడమ వైపు) 'నాట్ – సెక్యూర్' అని వస్తుంటుందని, అలా లేకపోయినా అడ్రస్ బార్‌లో ఉన్న వివరాల ఆధారంగా నకిలీదని గుర్తించాలని సూచిస్తున్నారు. ఇలాంటివి గమనించకుండా ముందుకు వెళితే నష్టపోవాల్సివస్తుందని హెచ్చరిస్తున్నారు.

ప్రభుత్వ వెబ్‌సైట్ అను నకిలీవి సృష్టించి మోసాలకు పాల్పడుతున్న నేపథ్యంలో ప్రజలు అప్రమత్తంగా ఉండాలి.

సాధారణ మెసేజ్‌లు, వాట్సాప్, ఫేస్‌బుక్, ఇతర సోషల్ మీడియా వ్యక్తిగత మెసెంజర్లకు వచ్చే వెబ్‌సైట్ (డొమైన్) లింకులను క్లిక్ చేయొద్దు. ఈ విషయాలపై అనుమానం, సందేహాలు ఉంటే సైబర్ క్రైమ్ పోలీసులను సంప్రదించాలి.

ప్రభుత్వ వెబ్‌సైట్‌కు సంబంధించిన లింక్‌లతో కూడిన మెసేజ్‌లు రావు. ఇలాంటి మెసేజ్‌లు వస్తే అవి సైబర్ మోసగాళ్ళవని భావించాలి.

ఇన్‌కంట్యాక్స్, జీఎస్టీ, ఇతర ట్యాక్స్‌లకు సంబంధించిన రీఫండ్ అంటూ వెబ్‌సైట్ లింకులతో ఎలాంటి మెసేజ్‌లు వచ్చినా పోలీసులకు సమాచారం అందించాలి.

Chittoor Police 9440900005

29. విదేశాల నుంచి మాట్లాడినట్లు సృష్టి - వాట్సాప్ వేదికగా సైబర్ మోసాలు

ఓ మధ్యతరగతి వ్యక్తి సెల్‌ఫోన్‌కు ఓ అపరిచితుడు వాట్సాప్ కాల్ చేశాడు. ఆ నంబరు +92తో ప్రారంభమైంది. అది పాకిస్తాన్‌లోని సెల్‌ఫోన్లకు వినియోగించే నంబరు.

కౌన్ బనేగా కరోడ్‌పతి లాటరీ గెలిచినందుకు రూ.3.5 కోట్లు ఇస్తామంటూ అపరిచితుడు ఆశపెట్టాడు.

అందుకు ప్రాసెసింగ్ రుసుము, ఆర్.బి.ఐ. క్లియరెన్స్, ఆదాయపన్ను చెల్లింపు కోసమంటూ రూ.4.5 లక్షలను పలు బ్యాంకు ఖాతాల్లోకి వేయమని సూచించాడు.

తరువాత తాము మోసపోయినట్లు తెలుసుకున్న బాధితురాలి ఫిర్యాదు మేరకు ప్రాథమికంగా దర్యాప్తు చేసిన పోలీసులు బీహార్‌లోని బ్యాంకు ఖాతాలకు డబ్బులు బదిలీ అయినట్లు గుర్తించారు.

సైబర్ నేరస్తుడు దేశంలోనే ఏదో ఓ ప్రాంతం నుంచి మాట్లాడతాడు... బాధితుడి సెల్‌ఫోను తెరపై మాత్రం విదేశాలకు చెందిన నంబర్లు ప్రత్యక్షమవుతాయి.

విదేశాలనుంచి మాట్లాడినట్లు నమ్మించి డబ్బులు కొల్లగొట్టేస్తారు :

వాట్సాప్ వేదికగా సరికొత్త తరహాలో మోసాలకు పాల్పడుతుండటం ఆందోళన కలిగిస్తోంది.

అమెరికా, లండన్, దుబాయ్, పాకిస్థాన్... ఇలా ఏదో ఒక దేశం నుంచి ఫోన్ వస్తునట్లు భ్రమించేందుకు నేరగాళ్ళు వాట్సాప్ కాల్, సందేశాలను వినియోగించుకుంటున్నారు.

బాధితుల్ని సులభంగా మోసగించడంతో పాటూ పోలీసుల దర్యాప్తును దారి మళ్ళించడానికి నేరగాళ్ళు ఇలా సరికొత్త ఎత్తుగడలను ఎంచుకుంటున్నారు.

వాట్సాప్ కాల్స్ లేదా సందేశాలతో బాధితులకు గాలమేస్తున్నారు :

సాధారణంగా ఒక చరవాణిలో వాట్సాప్ యాప్‌ను నిక్షిప్తం చేసుకునేటప్పుడు పలు వివరాలను నమోదు చేయాల్సి ఉంటుంది.

ఆ వివరాల్లో వినియోగదారుడి సెల్‌ఫోన్ నంబర్ నమోదు కీలకం. ఆ సమయంలో వినియోగదారుడు ఏ నంబరు నమోదు చేస్తే అదే నంబరుకు వాట్సాప్ నిర్వాహకుల నుంచి కోడ్ సందేశం వస్తుంది.

యాప్ నిక్షిప్తం చేసుకున్న నంబరుతో సంబంధం లేకుండానే ఈ ప్రక్రియ జరిగిపోతుంది. అలా వాట్సాప్ నిర్వాహకుల నుంచి వచ్చిన కోడ్ నంబరును తిరిగి నమోదు చేస్తే యాప్ ఇన్‌స్టలేషన్ ప్రక్రియ పూర్తవుతుంది.

ఈ ఫీచర్‌ను వినియోగించుకొని సైబర్ నేరగాళ్లు మోసాలకు తెర తీస్తున్నారు.

యాప్‌ను నిక్షిప్తం చేసుకునే సమయంలో ఎక్కడో విదేశాల్లో ఉన్న తమ సన్నిహితుల నంబరును వాట్సాప్ నిర్వాహకులకు పంపిస్తున్నారు.

ఆ నంబరుకు వచ్చే కోడ్‌ను ఇక్కడి సెల్‌ఫోన్‌లో నమోదు చేసి యాప్‌ను ఇన్‌స్టాల్ చేసుకుంటున్నారు.

అనంతరం ఆ సెల్‌ఫోన్ నుంచి పంపే సందేశాలు, వాట్సాప్ కాలింగ్ విదేశీ నంబరుతోనే వచ్చినట్లు చేయగలుగుతున్నారు.

తప్పుడు నంబర్లతో బాధితుల్ని బురిడీ కొట్టిస్తున్న నేరగాళ్లు డబ్బుల్ని వేయించుకునేది మాత్రం ఇక్కడి ఖాతాల్లోనే కావడం గమనార్హం.

విదేశీ ఖాతాల్లోనే నగదు బదిలీ చేయడం అంత సులభం కాదు కాబట్టి ఇక్కడి ఖాతా నంబర్లను బాధితులకు చెబుతున్నారు.

సైబర్ నేరాల దర్యాప్తు క్రమంలో నేరస్థుడిని పట్టుకున్నా డబ్బు తిరిగి స్వాధీనం చేసుకునేది అంతంతమాత్రమే కావడంతో ముందే మోసపోకుండా జాగ్రత్తపడాలని పోలీసులు సూచిస్తున్నారు.


fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice


twitter.com/InfoSecAwa


http://infosecawareness.in


Dial - 100

Chittoor Police 9440900005

౩౦. లక్కీడ్రాలో ఎంపికయ్యారంటూ ఎర

ప్రజలకు చిరపరిచితమైన వెబ్‌సైట్లు... ఈ–కామర్స్ సంస్థలను ఉపయోగించుకుని సైబర్ నేరస్థులు బహుమతుల పేరిట మోసాలకు తెగబడుతున్నారు. వాటి ద్వారా వస్తువులు కొన్నవారిని లక్ష్యంగా చేసుకుని లక్షల రూపాయిలు దోచుకొంటున్నారు. లక్కీ డ్రాలో ఎంపికయ్యారని... నగదు బహుమతులు, కార్లు ఇస్తామంటూ ఫోన్లు చేసి ఆకర్షిస్తున్నారు.

తెలిసిన సంస్థలు కావడం, పైగా వాటి నుంచి వస్తువులు కొనుగోలు చేయడం, చరవాణి ద్వారా బ్యాంకు లావాదేవీలు నిర్వహించి ఉండటంతో ప్రజలు నేరస్థుల మాటలు నమ్ముతున్నారు. నిజంగానే తమకు డ్రా లో బహుమతులు వచ్చాయని భావించి... నిందితులు సూచించిన ఖాతాల్లో వారు కోరిన విధంగా నగదు జమ చేస్తున్నారు. ఆ తర్వాత మోసపోయామని తెలుసుకుంటున్నారు.

హ్యుందాయ్ క్రెటా వచ్చిందంటూ...

ఓ ఈ–కామర్స్ సంస్థలో వస్తువులు కొన్నందుకు రూ.18 లక్షల విలువైన కారు బహుమతిగా వచ్చిందంటూ ఒక ప్రైవేటు ఉద్యోగిని సైబర్ నేరస్థులు మోసం చేశారు. కారు అనగానే సంబరపడిన ఆ వ్యక్తి అందుకోసం తాను ఏం చేయాలని వారిని అడిగారు.

తొలుత నివాస ధ్రువీకరణ, గుర్తింపు కార్డులు, బ్యాంకు ఖాతా నంబరు, ఇతర వివరాలు పంపాలని కోరారు.

అనంతరం మీ ఇంటికి సమీపంలో సదరు కంపెనీ కార్ల షోరూం ఎక్కడ ఉందని అడిగారు. మరుసటి రోజు ఫోన్‌చేసి మీ పేరుపై క్రెటా వాహనాన్ని కొనుగోలు చేశామని, నాలుగు రోజుల్లో షోరూం నుంచి తీసుకోవచ్చని తెలిపారు.

ప్రాసెసింగ్ రుసుం చెల్లించాలని ... రూ.15 వేలు తాము సూచించిన ఖాతాలో జమ చేయాలన్నారు. ఆ డబ్బు జమ చేసిన అనంతరం ఆదాయపు పన్ను కట్టాలంటూ రూ.75 వేలు తీసుకున్నారు.

రిజిస్ట్రేషన్ కోసం మరో రూ.25 వేలు కావాలని కోరగా... ఆ సొమ్మునూ చెల్లించారు. అనంతరం షోరూంకు వెళ్లి కారు వివరాలు వాకబు చేయగా.. ఎవరూ బుక్ చేయలేదని అక్కడి సిబ్బంది చెప్పారు. తనకు ఫోన్ చేసిన వారిని సంప్రదించేందుకు ప్రయత్నించగా.. స్పందన లేదు. దీంతో ఆయన పోలీసులను ఆశ్రయించారు.

➢ లక్కీడ్రాలో గెలుపొందారు... కార్లు, డబ్బులిస్తామంటే కచ్చితంగా మోసమేనని గ్రహించండి. రూ.లక్షలు దోచుకునేందుకే నేరస్థులు ఇలా చేస్తున్నారు. పేటీఎం, నాప్తోల్, షాప్‌క్లూస్ వంటి సంస్థలు లక్కీడ్రాలు నిర్వహించవన్న వాస్తవాన్ని గుర్తించండి. ఎవరైనా బహుమతుల పేరుతో ఫోన్లు చేస్తే ... సైబర్ క్రైం పోలీసులకు సమాచారం ఇవ్వండి.





fb.com/infosecawarness
fb.com/CDACINDIA
fb.com/chittoordistrictpolice



twitter.com/InfoSecAwa



http://infosecawareness.in



Dial - 100

Chittoor Police 9440900005